应用数学丛书目录

第 一 批

1. z变换与拉普拉斯变换　　关肇直　王恩平编著
2. 常微分方程及其应用　　秦化淑　林正国编著
3. 实变函数论基础　　胡钦训　编著
4. 正交函数及其应用　　柳重堪　编著
5. 沃尔什函数与沃尔什变换　　关肇直　陈文德编著
6. 圆柱函数　　刘　颖　编著

第 二 批

1. 集合论　　程极泰　编著
2. 图论　　王朝瑞　编著
3. 概率论　　狄昂照　编著
4. 矩阵理论　　王耕禄　史荣昌编著
5. 复变函数论　　杨维奇　编著
6. 逼近论　　徐利治　周蕴时　孙玉柏　编著
7. 矢量与张量分析　　冯潮清　赵愉深　何浩法　编著
8. 应用泛函分析　　柳重堪　编著

第 三 批

1. 网络理论　　张正寅　编著
2. 线性系统与多变量控制　　叶庆凯　编著
3. 椭圆函数及其应用　　高本庆　编著
4. 拓扑理论及其应用　　王则柯　凌志英　编著
5. 数理逻辑　　沈百英　编著

*6. 误差理论与数据处理　　贾沛璋　编著

7. 随机过程理论及应用　　熊大国　编著
8. 线性估计与随机控制　　卢伯英　陈宗基　编著

9．渐近分析方法及应用	徐利治　陈文忠	编著
10．预测的数学方法	张有为	编著
11．变分法及其应用	叶庆凯　郑应平	编著
12．应用离散数学	陈文德	编著
13．多项式与多项式矩阵	王恩平　王朝珠	编著
14．群论	刘木兰　冯克勤	编著

* 表示即将出版的书目。

出版说明

近二十年来电子工程、控制工程、系统工程及其它领域都获得巨大发展。众所周知，这些科学技术研究的发展是与现代逐渐形成的应用数学学科紧密相联，相辅相成。尤其近年发展起来的边缘学科，更是与数学紧密结合。但一般数学专著比较偏重于论证严谨，全面系统，篇幅较大，理论较深。广大科技工作者学习此类著作，往往需时较多，与工作结合不紧，收效不大。本丛书将为目前在电子工程、控制工程、系统工程等领域工作的同志在数学基础的提高上，提供适合其工作特点的数学参考书。

本丛书是一种介于现代应用数学专著与工程专业理论书籍之间的桥梁参考著作。更着重于科技工作中应用较多的数学概念，分析和解题的基本技巧。也包括一部分适合于实际工作者为学习更高深的现代应用数学专著所需之基础知识。

本丛书选材包括三个方面：基础数学；应用数学有关领域的基础介绍；应用于科技中的典型基础专业理论。出版采用分册形式。各册内容独立，自成系统，但仍有少量交叉，分期分批出版。

丛书可供大专院校有关专业研究生、教师、从事科研生产的工程师参考。

前 言

群论是从实践中发展起来的一门比较抽象的学科，它不仅在数学中居显著地位，而且在许多现代科学分支中居重要地位。群论的概念和结果远不限于对几何学、拓扑学等纯粹数学方面的应用，实际上它已成为研究物质结构和物质微粒运动的有力工具。随着科学技术的发展，群论的理论和方法获得了愈来愈广泛的应用，除了大家比较熟悉的对物理学、特别是理论物理学和结晶学的应用，它还渗透到计算机科学，通讯理论，系统科学、乃至数理经济等许多领域。因此，今天需要掌握和了解群论知识的人愈来愈多。然而，由于这一学科的高度抽象，尽管国内外关于群论的专著和教材很多，但是多数论著和教材对非数学工作者，甚而对应用数学工作者来说都不易接受，往往是学习了一系列的名词、定义和定理之后不知如何使用。我们撰写本书的目的就是尝试解决这一矛盾。我们在讲述基本概念时，尽量配合较多的简单具体的例子，希望读者获得一些感性认识。为了避免学过群论之后，而对具体问题无从下手的弊病，我们采取对典型例子进行详细讨论，并给出具体计算，从而使读者掌握一些群论计算的技巧和分析问题的方法。

本书的内容分两大部分。第一部分由前三章组成，主要介绍群论的基本概念和结果。为了使读者加深对基本概念的理解和学习运用群论的一般结果来讨论具体问题，我们详细地论述了低阶群的结构。第二部分由后二章组成，主要介绍点群和域上典型群的结构。在一般群论的教材中通常不包含这部分内容。实际上，点群对几何学、结晶学和理论物理的应用是相当精彩的。至于典型群，不管是从它对几何学、物理学的应用角度来看，还是从群论本身的研究来看，它在群论中都占有重要地位。鉴于本书的目

的和读者对象，它没有包含像连续群，群表示论等重要内容，对连续群有兴趣的读者可参见参考文献〔11〕，对群表示论有兴趣的读者可参见参考文献〔2〕。

最后，作者感谢汪栋臣同志对本书的出版给予的热情帮助。由于作者水平有限，谬误一定不少，敬请读者批评指正。

作　者

目　　录

第一章　群和它的基本性质 …… 1
§1.1　集合论的预备知识 …… 1
§1.2　什么是群 …… 9
§1.3　子群和陪集分解 …… 14
§1.4　循环群 …… 22
§1.5　正规子群　商群　同态定理 …… 26
第二章　群在集合上的作用　西洛（Sylow）定理 …… 32
§2.1　置换群 …… 32
§2.2　群在集合上的作用 …… 37
§2.3　西洛定理 …… 44
第三章　群的结构 …… 50
§3.1　自由群和群的表现 …… 50
§3.2　有限生成阿贝尔群结构 …… 57
§3.3　小阶群的结构 …… 64
§3.4　幂零群和可解群 …… 76
第四章　有限点群 …… 85
§4.1　三维空间中的正交群 …… 85
§4.2　欧几里得群 …… 92
§4.3　$E(3)$的离散子群 …… 96
§4.4　正多面体和它们的对称群 …… 100
§4.5　第一类点群 …… 108
§4.6　第二类点群 …… 116
§4.7　晶体点群 …… 118
第五章　典型群 …… 124
§5.1　线性群的结构 …… 124
§5.2　双线性型 …… 138
§5.3　交错型 …… 143
§5.4　辛群 …… 145
§5.5　二次型和对称双线性型 …… 167
§5.6　正交群 …… 172
参考文献 …… 189

第一章　群和它的基本性质

§1.1　集合论的预备知识

群是集合上赋予具有某些性质的二元运算的一种代数结构，所以在讲述什么是群之前，需要介绍集合论中我们今后所需要的一些预备知识。

一些特定的对象放在一起就叫作一个**集合**。例如全体自然数构成一个集合，叫作自然数集合，表示成$\mathbb{N}$。全体整数构成整数集合，表示成$\mathbb{Z}$。类似地有有理数集合，实数集合，复数集合，分别表示成$\mathbb{Q}$，$\mathbb{R}$，$\mathbb{C}$。集合A中的每个对象a叫作是A的**元素**，表示成$a\in A$，说成元素a**属于**集合A。否则，若a不属于集合A，则表成$a\notin A$。设A和B是两个集合，如果A中每个元素均为B中的元素，即

$$a\in A\Rightarrow a\in B$$

则称A是B的一个**子集**，表示成$A\subseteq B$，或者$B\supseteq A$。如果$A\subseteq B$，并且$B\subseteq A$，即A中元素均是B中元素，反之亦然，于是

$$a\in A\Longleftrightarrow a\in B$$

这也相当于集合A和B包含同样的元素。这时，便称集合A和B相等，表示成$A=B$。如果A是B的子集，并且不等于B（即$A\subseteq B$，$A\neq B$），则称A是B的**真子集**，表示成$A\subset B$或者$B\supset A$。不包含任何元素的集合叫作**空集**，表示成$\varnothing$。于是空集是每个集合的子集。

可以有许多方法来表达一个确定的集合。例如若集合A只有有限多个元素a_1，a_2，…，a_n（n是自然数），我们可以把这几个元素全列出来加上括号｛　｝来表示这个集合，即$A=\{a_1, a_2, \cdots, a_n\}$，只有有限多元素的集合叫**有限集**，否则叫**无限集**，具有n个元素的集合也叫**n元集合**，元素个数n叫作有限集A的**势**，表

示成$|A|=n$。在一般情形下，集合S中具有某个性质P的元素构成的集合通常表成

$$\{x\in S\mid x\text{有性质}P\}$$

例如：偶数集合$\{0,\ \pm 2,\ \pm 4,\ \cdots\}$可以表成$\{n\in\mathbb{Z}\mid z\mid n\}$，而奇自然数集合$\{1,\ 3,\ 5,\ 7,\cdots\}$可以表成$\{n\in\mathbb{Z}\mid 2\nmid n,\ n\geqslant 1\}$（这里$2\mid n$表示2整除$n$，$2\nmid n$表示2不整除$n$）。

由一些已知的集合构作新的集合通常用集合的运算来实现的。下面是集合的一些最基本的运算。设A和B是两个集合，它们的公共元素所构成的集合叫作A和B的**交**，表示成$A\cap B$。于是，$A\cap B=\{x\mid x\in A\text{并且}x\in B\}$。类似地，$n$个集合$A_1,\cdots,A_n$的交是

$$A_1\cap A_2\cap\cdots\cap A_n=\bigcap_{i=1}^{n}A_i=\{x\mid x\in A_i(1\leqslant i\leqslant n)\}$$

更一般地，对于任意多个集合形成的集族$\{A_i\mid i\in I\}$（其中I是一个集合，叫该集族的**指标集合**，对于每个$i\in I$，A_i是该集族中的一个集合），它的交为

$$\bigcap_{i\in I}A_i=\{x\mid x\in A_i(\text{对每个 }i\in I)\}$$

第二个运算是一些集合的**并**，集合A和B的并表示成$A\cup B$，定义为$A\cup B=\{x\mid x\in A\text{或者}x\in B\}$。类似地，

$$A_1\cup A_2\cup\cdots\cup A_n=\bigcup_{i=1}^{n}A_i=\{x\mid x\in A_i(\text{对某个 }i,1\leqslant i\leqslant n)\}$$

一般地，集族$\{A_i\mid i\in I\}$的并是

$$\bigcup_{i\in I}A_i=\{x\mid x\in A_i(\text{对某个 }i\in I)\}$$

练习1.1.1 设B，$A_i(i\in I)$均是集合，则

$$B\cap\left(\bigcup_{i\in I}A_i\right)=\bigcup_{i\in I}(B\cap A_i),$$

$$B\cup\left(\bigcap_{i\in I}A_i\right)=\bigcap_{i\in I}(B\cup A_i)。$$

设A是B的子集，令$B-A=\{x\mid x\in B,\ x\notin A\}$，叫作是子集$A$关于$B$的**补集**。如果在讨论问题时所涉及的集合$A$，$B$，$C$，…均是某个大集合$\Omega$的子集，则$\Omega-A$简称作$A$的补集，表示作$\bar{A}$。

练习1.1.2 求证

$$\overline{\bigcup_{i\in I}A_i}=\bigcap_{i\in I}\bar{A}_i,\quad \overline{\bigcap_{i\in I}A_i}=\bigcup_{i\in I}\bar{A}_i。$$

设A和B是两个集合，我们把集合

$$\{(a,\ b)\mid a\in A,\ b\in B\}$$

叫作是A和B的**直积**，表示成$A\times B$。若$(a,\ b)$，$(a',\ b')\in A\times B$，则$(a,\ b)=(a',\ b')$当且仅当$a=a'$，并且$b=b'$。类似地可定义n个集合A_1，A_2，…A_n的直积

$$A_1\times A_2\times\cdots\times A_n=\prod_{i=1}^{n}A_i=\{(a_1,\ \cdots,\ a_n)\mid a_i\in A_i(1\leqslant i\leqslant n)\}。$$

更一般地，集族$\{A_i\mid i\in I\}$的直积定义为

$$\prod_{i\in I}A_i=\{(a_i)_{i\in I}\mid a_i\in A_i(对每个\ i\in I)\}。$$

为了比较不同的集合，我们需要使不同的集合之间发生联系，这就是从一个集合到另一集合的映射。f叫作从集合A到集合B的映射，是指对于A中每个元素a，均有确定的办法给出集合B中唯一的一个对应元素，这个对应元素记成$f(a)$，叫作a在映射f之下的像，而f把a映成$f(a)$这件事表示成$a\mapsto f(a)$。从A到B的映射f表示成f：$A\to B$或者$A\xrightarrow{f}B$。

设f：$A\to B$和g：$B\to C$都是集合之间的映射。对于每个元素$a\in A$，f把它映成B中元素$f(a)$，然后g又把$f(a)$映

成C中元素$g(f(a))$。由此得到一个从A到C的映射$a \mapsto g(f(a))$。这个映射叫作是f与g的合成，表示成$g \circ f: A \to C$

设f和g均是从集合A到集合B的映射，称f和g相等（表示成$f = g$），是指对于每个元素$a \in A$，均有$f(a) = g(a)$。现在我们证明映射的合成运算满足结合律。

引理1.1.1 设$f: A \to B$，$g: B \to C$，$h: C \to D$均是集合的映射，则$h \circ (g \circ f) = (h \circ g) \circ f$。

证明 对于$a \in A$，令$f(a) = b$，$g(b) = c$，$h(c) = d$，则$(g \circ f)(a) = c$，$(h \circ g)(b) = d$。于是$h \circ (g \circ f)(a) = h(c) = d$，$((h \circ g) \circ f)(a) = (h \circ g)(f(a)) = (h \circ g)(b) = d$，即对于$A$中每个元素$a$，均有$(h \circ (g \circ f))(a) = ((h \circ g) \circ f)(a)$，从而$h \circ (g \circ f) = (h \circ g) \circ f$。证毕。

设$f: A \to B$是集合的映射，对于A的每个子集A'，令$f(A') = \{f(x) | x \in A'\}$，这是$B$的子集，叫作$A'$在$f$之下的**像**。对于$B$的每个子集$B'$，令$f^{-1}(B') = \{x \in A | f(x) \in B'\}$，这是$A$的子集，叫$B'$的**原像**。如果$f(A) = B$，即$B$中每个元素均是$A$中某元素在$f$之下的像，便称$f$是**满射**。另一方面，如果$A$中不同元素在$f$之下映成不同的像元素，即$a, a' \in A$，$a \neq a' \Rightarrow f(a) \neq f(a')$，则称$f$为**单射**。如果$f: A \to B$同时是单射和满射，则称$f$为**一一映射**或者**一一对应**。最简单的例子是：将集合A中每个元素均映成自身的映射$1_A: A \to A$，就是A到A的一一对应，映射1_A叫作集合A上的**恒等映射**，通常采用下面引理来判断一个映射是否为一一对应。

引理1.1.2 映射$f: A \to B$是一一对应的充分必要条件是存在映射$g: B \to A$，使得$f \circ g = 1_B$，$g \circ f = 1_A$。

证明 如果f是一一对应，根据定义这意味着对于B中每个元素b，均有唯一的原像$a = f^{-1}(b)$，于是可以定义映射$g: B \to A$，$g(b) = f^{-1}(b)$，直接验证$g \circ f = 1_A$和$f \circ g = 1_B$成立。另一方面，如果f不是满射，则存在$b \in B$，使$f^{-1}(b) = \varnothing$。因此对每个映射$g: B \to A$，均有$(f \circ g)(b) = f(g(b)) \neq b$，因

此$f\circ g\neq 1_B$。如果f不是单射，则存在a，$a'\in A$，$a\neq a'$,使得$f(a)=f(a')$。记这个B中元素为b，那么对于每个映射$g:B\to A$，

$(g\circ f)(a)=g(b)=(g\circ f)(a')$，这就表明$g\circ f\neq 1_A$。因此，若存在$g:B\to A$，使得$f\circ g=1_B$，并且$g\circ f=1_A$，则$f$必然是一一对应。证毕。

注记1.1.1 当f：$A\to B$是一一对应时，满足$f\circ g=1_B$和$g\circ f=1_A$的映射$g:B\to A$是唯一存在的，这是因为若$g':B\to A$,也有性质$f\circ g'=1_B$，$g'\circ f=1_A$,则$g'=g'\circ 1_B=g'\circ(f\circ g)=(g'\circ f)\circ g=1_A\circ g=g$。我们将这个唯一存在的映射$g$叫作$f$的**逆映射**，表示成$f^{-1}$。

练习1.1.3 设f：$A\to B$是集合的映射，A是非空集合，则

(a) f为单射$\Longleftrightarrow$存在$g:B\to A$，使得$g\circ f=1_A$。

(b) f为满射$\Longleftrightarrow$存在$h:B\to A$，使得$f\circ h=1_B$，并用此结果证明引理1.1.2。

练习1.1.4 如果$f:A\to B$，$g:B\to C$均是一一对应,求证$g\circ f$：$A\to C$也是一一对应，并且$(g\circ f)^{-1}=f^{-1}\circ g^{-1}$。

设A是一个集合，则积集$A\times A$的每个子集R叫作集合A的一个**关系**。如果$(a,b)\in R$，便称a和b有关系R，写成$a\underset{R}{\sim}b$。例如对于集合

$$R=\{(a,b)\in \mathbb{R}\times\mathbb{R}\mid a\text{比}b\text{大}\},$$

则实数a和b有关系R即意味着a比b大。这就是“大于”关系，通常将这个关系表成$a>b$。同样地实数集合上还有关系$\geqslant$（大于或等于）$<$(小于)，$\leqslant$(小于或等于)，$=$(等于)。集合A上的关系$\sim$叫作**等价关系**，是指它满足如下三个条件

(1) 自反性：$a\sim a$(对每个$a\in A$)；

(2) 对称性：若$a\sim b$，则$b\sim a$；

(3) 传递性：若$a\sim b$，$b\sim c$，则$a\sim c$。

设$\sim$是集合A上的等价关系。如果$a\sim b$，则由对称性知

$b\sim a$，这时，称元素 a 和 b **等价**。对于每个 $a\in A$，以 $[a]$ 表示 A 中与 a 等价的全部元素构成的集合，即

$$[a]=\{b\in A \mid b\sim a\}。$$

由自反性可知 $a\in[a]$，而 $[a]$ 叫作 a 所在的**等价类**。由传递性可知，每个等价类中任意两个元素均彼此等价（设 $b, c\in[a]$，则 $b\sim a$，$a\sim c$，于是 $b\sim c$）。进而，对于 a，$b\in A$，如果 $a\sim b$，则 $[a]=[b]$；如果 $a\nsim b$（表示 a 和 b 不等价），则 $[a]\cap[b]=\varnothing$，即 $[a]$ 和 $[b]$ 不相交（请读者证明）。于是任意两个等价类或者相等，或者不相交。再由于 A 中每个元素 a 均属于等价类 $[a]$，综合上述，可知集合 A 是一些等价类 $\{[a_i] \mid i\in I\}$ 的并，而这些等价类是两两不相交的。每个等价类 $[a_i]$ 中取出一个元素 a_i，则 $R=\{a_i \mid i\in I\}$ 具有如下的性质：A 中每个元素均等价于某个 a_i，而不同的 a_i 彼此不等价。我们把具有这样性质的 R 叫作是 A 对等价关系 $\sim$ 的一个**完全代表系**。于是

$$A=\bigcup_{a\in R}[a]\text{(非交并)} \qquad (*)$$

一般地，若集合 A 是它的某些子集 $\{A_i \mid i\in I\}$ 的**非交并**，即 $A=\bigcup\limits_{i\in I}A_i$，并且不同的 A_i 两两不相交，我们便称 $\{A_i \mid i\in I\}$ 是 A 的一个**分拆**。如上所述，A 上的每个等价关系均给出集合 A 的一个分拆（$*$）。反过来，如果 $\{A_i \mid i\in I\}$ 是集合 A 的一个分拆，可以如下定义集合 A 上的一个关系：对于 a，$b\in A$，

$a\sim b\Longleftrightarrow a$ 和 b 在同一个 A_i 之中（对某个 $i\in I$）。请读者验证这是一个等价关系。以 E 表示集合 A 的全部等价关系，以 P 表示 A 的全部分拆，则上述给出从等价关系到分拆的一个映射 $f: E\to P$ 和从分拆到等价关系的一个映射 $g: P\to E$。请读者证明 f 和 g 是互逆的，即 $f\circ g=1_P$，$g\circ f=1_E$，从而 f 是一一对应（引理1.1.2）。换句话说，集合 A 上的等价关系和 A 的分拆是一一对应的。

例如　设P是由某些集合构成的集族，在P上定义如下的关系：对于A，$B\in P$，

$A\sim B\Longleftrightarrow$存在着从集合$A$到集合$B$的一一对应。

这是P上的一个等价关系（自反性：1_A：$A\rightarrow A$是一一对应，从而$A\sim A$；对称性：若f：$A\rightarrow B$是一一对应，则f^{-1}：$B\rightarrow A$亦然，从而$A\sim B\Rightarrow B\sim A$；传递性：基于练习1.1.4），从而$P$由此分拆成一些等价类的非交并，彼此等价的集合叫作是**等势的**。比如说：两个有限集A和B等势当且仅当它们的元素个数相同，即$|A|=|B|$。与自然数集合$\mathbb{N}=\{1,2,\cdots,n,\cdots\}$等势的集合叫作**可数无限集合**，其他无限集则叫作是**不可数集合**。熟知实数集合是不可数的，而偶自然数集合$\{2,4,\cdots,2n,\cdots\}$是可数集合，因为存在着它到自然数集合$\mathbb{N}$的一一对应$2n\mapsto n$。这个例子也表明：无限集合A的一个真子集可以与A等势！请读者证明。

练习1.1.5　证明

（a）每个无限集均包含一个可数无限子集。

（b）集合A是无限的$\Longleftrightarrow A$和它的某个真子集等势。

练习1.1.6　设A是有限集，$P(A)$是A的全部子集（包括空集）所构成的集族，求证$|P(A)|=2^{|A|}$。换句话说，n元集合共有2^n个不同的子集。

练习1.1.7　设A_1，…，A_n均是有限集，则

$$|A_1\times\cdots\times A_n|=|A_1|\cdots|A_n|。$$

若集合A和A上的二元关系$a\geqslant b$满足下面的性质：

（1）自反性：$a\geqslant a$；

（2）反对称性：若$a\geqslant b$和$b\geqslant a$，则$a=b$；

（3）传递性：若$a\geqslant b$，$b\geqslant c$，则$a\geqslant c$。则称A为**偏序集**。

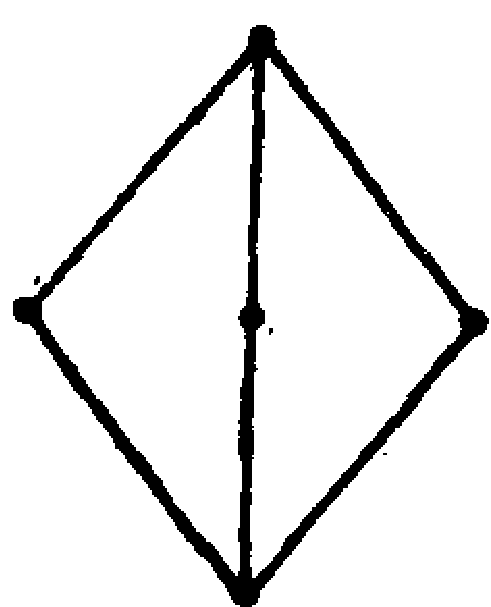
一般来说，集合A中的2个元素a和b，可能既没有关系$a\geqslant b$，也没有关系$b\geqslant a$。若A中任何二个元素a和b，总有$a\geqslant b$或者$b\geqslant a$，则称A为**全序集**。例如，我们熟悉的自然数集合，实数集合，按通常数的大小关系成为全序集。集合A的所有子集的集合$P(A)$，按集合的包含定义二元关系，则$P(A)$是

一个偏序集。

偏序集A的元素u称为A的子集A_1的**上界**，如果对每个$a\in A_1$，都有$u\geqslant a$，元素u称为A_1的**最小上界**。如果u是A_1的上界，且对A_1的任何上界v，均有$u\leqslant v$。显然，如果最小上界存在必唯一。类似地可以定义下界和最大下界。偏序集A的元素l称为子集B的**下界**，如果对每个$b\in B$，都有$l\leqslant b$（即$b\geqslant l$）；元素l为B的最大下界，如果l是B的下界，而且对B的任一下界m，均有$l\geqslant m$。如果最大下界存在必定是唯一的。例如$P(A)$，子集A_1和A_2的最小上界是$A_1\cup A_2$，最大下界是$A_1\cap A_2$。

在偏序集A中，我们说元素a_1是a_2的**覆盖**，如果$a_1>a_2$，而且不存在元素u使得$a_1>u>a_2$。在有限偏序集中，$a>b$当且仅当存在序列$a_1=a$，a_2，…，$a_n=b$，使得每个a_i是a_{i+1}的覆盖。可以用图表示有限偏序集A。用平面上的点表示A的元素，和如果a_1是a_2的覆盖，将a_1放在a_2的上面，同时用直线段联结a_1和a_2。因此，$a<b$当且仅当存在a到b的折线。如果在a和b（$\neq a$）之间没有线段相连，则表示a和b不可比较，即a和b没有关系。下面的几个图均表示偏序集。

偏序集A，如果它的任何2个元素都有最小上界和最大下界，则称A为格。图1-1图1-2和图1-3都是格，图1-3是一个全序集，而图1-4只是偏序集而不是格。


图 1-1

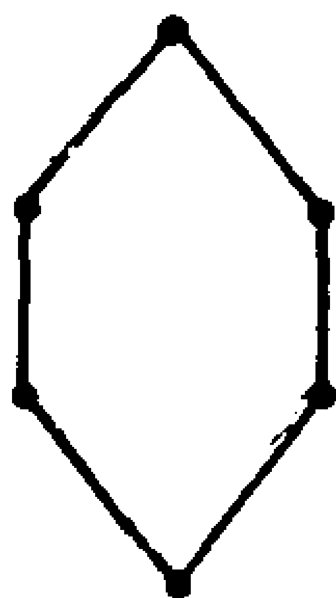
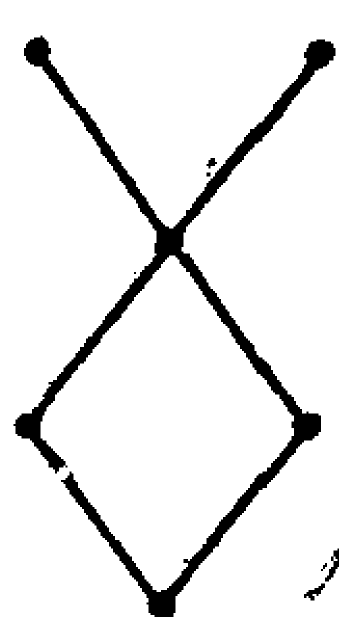

图 1-2


图 1-3


图 1-4

设A是一个集合，则从$A\times A$到A的每个映射$f: A\times A\to A$叫作集合A上的一个(二元)运算。例如：通常的整数加法就是运算$f: \mathbb{Z}\times\mathbb{Z}\to\mathbb{Z}$，其中$f(m, n)=m+n$。类似地，整数

的减法和乘法也是$\mathbb{Z}$上的运算。我们往往把集合A上的运算表示成·，即对于$a, b \in A$，$f(a, b)$写成$a \cdot b (\in A)$，或者简单地写成ab。

运算·叫作满足结合律，如果对任意$a, b, c \in A$，有$a \cdot (b \cdot c) = (a \cdot b) \cdot c$。运算·叫作满足**交换律**，如果对任意$a, b \in A$，有$a \cdot b = b \cdot a$。一个集合赋予满足某些特定性质的（一个或多个）二元运算，便得到各种代数结构。本书则讲述一种代数结构——群，先从半群讲起。

§1.2 什么是群

定义1.2.1 一个**半群**是指一个集合S和集合S上满足结合律的一个（二元）运算。这个半群可表示成$(S, \cdot)$，或者当运算很明确的时候，简记成S，而运算$x \cdot y$也可简记成xy。

如果运算又满足交换律，则$(S, \cdot)$叫作**交换半群**。像通常那样，令$x^2 = x \cdot x$，$x^{n+1} = x^n \cdot x (= x \cdot x^n)(n \geqslant 1)$。

定义1.2.2 设S是一个半群，元素$e \in S$，e叫作是半群S的**幺元素**或单位元，是指对每个$x \in S$，$xe = ex = x$。

如果半群S具有幺元素，则它是唯一的。因为若e'也是半群S的幺元素，则$e = ee' = e'$。我们将半群S中这个唯一的幺元素（如果存在的话）通常记成1_S，或者简记成1。具有幺元素的半群叫作**含幺半群**。

定义1.2.3 设S是含幺半群，元素$x \in S$叫作元素$y \in S$的**逆元素**，是指$xy = yx = 1$。

如果元素x具有逆元素，则它一定是唯一的。因为若y'也是x的逆元素，则$xy' = y'x = 1$，于是$y = y \cdot 1 = y(xy') = (yx)y' = 1 \cdot y' = y'$。所以若$x$具有逆元素，我们把这个唯一的逆元素表示成$x^{-1}$。因此，$xx^{-1} = x^{-1}x = 1$。

练习1.2.1 设S是含幺半群，$x, y \in S$。

(a) 如果x具有逆元素，则x^{-1}也有逆元素，且$(x^{-1})^{-1} = x$。

(b) 如果 x 和 y 均具有逆元素，则xy也有逆元素，并且 $(xy)^{-1}=y^{-1}x^{-1}$。

(c) $1^{-1}=1$。

定义1.2.3 半群G如果有幺元素，并且每个元素均可逆，则G叫作**群**。此外，如果运算又满足交换律，则G叫作**交换群**，或叫**阿贝尔(Abel)群**。

下面给出半群和群的一些例子。

例1.2.1 设M为非负整数全体，则$(M, +)$是含幺交换半群，幺元素是数0，但它不是群，因为只有0对于加法在M中才是可逆的。$(\mathbb{Z}, +)$，$(\mathbb{Q}, +)$，$(\mathbb{R}, +)$，$(\mathbb{C}, +)$均是阿贝尔群，幺元素为0，数a的逆元素是$-a$。它们分别叫作整数加法群，有理数加法群等等。

$(\mathbb{N}, \times)$是含幺交换半群，幺元素为1，它不是群，因为只有1对于乘法在自然数集合中才可逆。令$\mathbb{Q}^*$表示非零有理数全体，则$(\mathbb{Q}^*, \times)$是交换群。幺元素为1，非零有理数a的乘法逆元素为a^{-1}，这叫有理数乘法群。同样的，非零实数（复数）全体构成实数（复数）乘法群。所有这些群都是阿贝尔群。

例1.2.2 以$M_{m,n}(\mathbb{C})$表示全部m行n列的复数矩阵组成的集合，它对矩阵加法形成交换群。幺元素是全零矩阵，而矩阵$A=(a_{ij})$的加法逆是$-A=(-a_{ij})$。以$M_n(\mathbb{C})$表示n阶复方阵组成的集合，它对于乘法形成含幺半群。幺元素是单位矩阵I_n。由线性代数可知，n阶复方阵A有乘法逆的充分必要条件是$\det A\neq 0$，即A是非异方阵。$M_n(\mathbb{C})$不是群，并且当$n\geqslant 2$时，易知半群$M_n(\mathbb{C})$不是交换的。我们还可以将$\mathbb{C}$改成$\mathbb{R}$，$\mathbb{Q}$，$\mathbb{Z}$，而得到加法交换群$M_{m,n}(\mathbb{R})$，含幺半群$M_n(\mathbb{R})$等等。

例1.2.3 设A是非空集合，以$\Sigma(A)$表示从A到A的全体映射所构成的集合，则$\Sigma(A)$对于映射的合成运算形成含幺半群。幺元素是恒等映射1_A。由引理1.1.2可知，$\Sigma(A)$中映射f：$A\to A$可逆的充要条件是f为一一对应，所以当集合A有多于1个元素时，$\Sigma(A)$不是群，并且半群$\Sigma(A)$不是交换的。

例1.2.4 欧氏平面$\mathbb{R}^2$中保持欧氏距离不变的运动叫作**欧氏运动**。由于每个欧氏运动均是$\mathbb{R}^2$上的一一对应，并且它的逆仍是欧氏运动，而两个欧氏运动合成的结果仍是欧氏运动，从而全部欧氏运动形成群，叫作**欧氏平面的运动群**，这也是非交换群。

例1.2.5 设n为正整数，在整数集合$\mathbb{Z}$上定义如下的关系：对于整数a和b，$a \sim b \Longleftrightarrow n \mid a-b$，用初等数论中的同余符号，则$a \sim b$相当于$a \equiv b \pmod n$。易知这是一个等价关系，并且整数集合$\mathbb{Z}$分拆成$n$个等价类$\bar{0}$，$\bar{1}$，…，$\overline{n-1}$之并，其中$\bar{i}$表示整数$i$所在的等价类。而$\{0, 1, 2, \cdots, n-1\}$是整数对于上述模$n$同余关系的一个完全代表系，以$Z_n$表示这$n$个等价类组成的集合。在其上定义加法

$$\bar{a}+\bar{b}=\overline{a+b}$$

由同余式的基本性质可知，这个加法运算是可以定义的，即与等价类（或叫模n同余类）中代表元素的取法无关，并且Z_n对于这个运算形成交换群，幺元素是$\bar{0}$，叫作**整数模n加法群**。如果在Z_n中定义乘法$\bar{a}\bar{b}=\overline{ab}$，则$Z_n$对此乘法是含幺交换半群，幺元素为$\bar{1}$。由于等式$\bar{a}\bar{b}=\bar{1}$相当于同余式$ab \equiv 1 \pmod n$，从初等数论知道，对于给定的$a$，存在$b$满足此同余的充分必要条件是$a$与$n$互素，从而$\bar{a}$对于乘法是可逆元素的充要条件是$(a, n)=1$。设$(M, \cdot)$是一个含幺半群，而以$\cup(M)$或者$M^*$表示半群$M$中可逆元素全体。

定理1.2.1 如果$(M, \cdot)$是含幺半群，则$(\cup(M), \cdot)$为群。

证明 由于$1_M^{-1}=1_M$，从而$1=1_M \in \cup(M)$。对于$a, b \in \cup(M)$，即a，b均可逆，于是ab也可逆（因为$b^{-1}a^{-1}$是它的逆元素）。从而$\cdot$是$\cup(M)$上的二元运算，它当然在$\cup(M)$中仍然满足结合律，于是$(\cup(M), \cdot)$是含幺半群。由于$\cup(M)$中每个元素a均可逆，且逆元素a^{-1}也可逆（$(a^{-1})^{-1}=a$），即$a^{-1} \in \cup(M)$。因此$\cup(M)$中每个元素在$\cup(M)$中均可逆，根据定义，$\cup(M)$是群。证毕。

由前面的例子可知：

（1）全体 n 阶可逆复方阵形成乘法群，叫作复数上的 n 次一般线性群，表示成 $GL(n, \mathbb{C})$，同样有 $GL(n, \mathbb{R})$ $GL(n, \mathbb{Q})$ 等。

（2）对于每个非空集合 A，A 到自身之上的所是一一对应对于合成运算形成群，这叫作集合 A 上的**全置换群或对称群**，表示成 $S(A)$，其中每个元素（即 A 到 A 的一一对应）叫作是集合 A 上的一个**置换**。

（3）设 n 为正整数，$\bar{a}$ 为整数 a 的模 n 同余类，则集合 $Z_n^* = \{\bar{a} | (a, n) = 1\}$ 对于乘法形成阿贝尔群。这个群熟知共有 $\varphi(n)$ 个元素，其中 $\varphi(n)$ 是初等数论中的欧拉函数。

设 G 是一个群，如果集合 G 是有限的，则 G 叫作**有限群**，否则叫**无限群**。如果有限群 G 共有 n 个元素，则 G 叫 **n 阶群** 或 **n 元群**，n 叫作有限群 G 的阶。

为了考查各种群之间的联系，需要研究群之间的映射，但是群除了是集合之外还有运算，所以我们需要映射与群的运算保持相容。确切地说，则有如下的定义。

定义1.2.4 设 $(G, \cdot)$ 和 $(G', \circ)$ 是两个群，映射 $f: G \to G'$ 叫作是群 G 到群 G' 的**同态**，是指对任意 $a, b \in G$，$f(a \cdot b) = f(a) \circ f(b)$（或者简记为 $f(ab) = f(a)f(b)$）。此外，如果 f 又是单射或满射，则 f 分别叫作**单同态**或**满同态**。如果同态 f 是一一对应，则称 f 是群 G 到群 G' 的**同构**，并且称 G 和 G' 是同构的，表示成 $G \cong G$，或者 $f: G \simeq G'$。

彼此同构的群具有完全相同的群的结构，在群论中，同构的群认为本质上是同一个群。我们更主要的是研究本质不同的群之间联系，所以同态是群论中一个最重要的研究工具。

例1.2.6 考虑映射 $\det$: $GL(n, \mathbb{C}) \to \mathbb{C}^*$，其中映射 $\det$ 将一般线性群 $GL(n, \mathbb{C})$ 中每个矩阵 A 映成它的行列式 $\det A$（这是非零复数乘法群 $\mathbb{C}^*$ 中的元素）。由线性代数知 $\det(AB) = (\det A)(\det B)$，从而 $\det$ 是群的同态，并且易知这是满同态，但

是当 $n\geqslant 2$ 时这不是单同态。

例1.2.7 设 n 为自然数，$C_n=\{e^{\frac{2\pi i}{n}a}\mid a=0, 1, 2, \cdots, n-1\}$，则 C_n 中 n 个复数对于乘法形成群，作映射 f：$C_n\to(Z_n, +)$，$e^{\frac{2\pi i}{n}a}\mapsto\bar{a}$，则 $f(e^{\frac{2\pi i}{n}a}\cdot e^{\frac{2\pi i}{n}b})=f(e^{\frac{2\pi i}{n}(a+b)})=\overline{a+b}=\bar{a}+\bar{b}=f(e^{\frac{2\pi i}{n}a})\cdot f(e^{\frac{2\pi i}{n}b})$。所以，$f$ 是群的同态。显然 f 是一一对应，从而 f 是群的同构。

如果 $n\geqslant 3$，考虑以点 o 为中心的正 n 边形(图1-5为 $n=6$ 的情形)。设 G_n 是将此正 n 边形变为自身的旋转群。如果以 σ 表示以点 o 为中心反时针方向旋转 $\frac{360^\circ}{n}$ 的旋转，则 $G_n=\{1, \sigma, \sigma^2, \cdots, \sigma^{n-1}\}$(注意 $\sigma^n=1(=\sigma^\circ)$)。不难看出，群 G_n 与前面的 C_n 和 Z_n 都是同构的，尽管它们分别来自几何，代数或者数论，但是在群论中，它们本质上是同一个群，即具有完全相同的群结构。

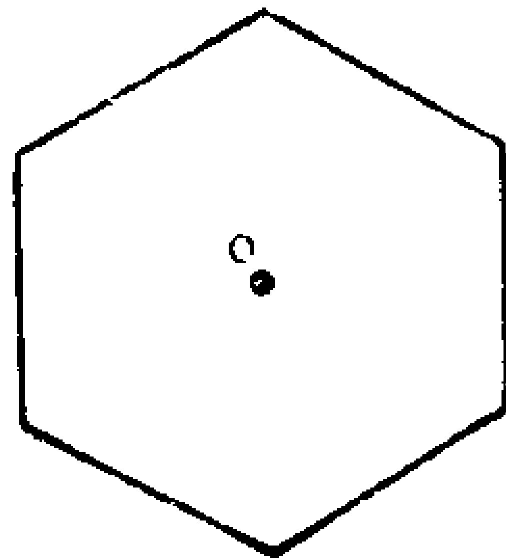


图 1-5

练习1.2.2(群中的消去律) 设 x，y，z 是群 G 中元素，如果 $xy=xz$ 或者 $yx=zx$，则 $y=z$。(提示：将等式两边左乘或者右乘以 x^{-1})。

练习1.2.3 设 f：$G\to G'$ 是群的同态，求证 $f(1_G)=1_{G'}$，并且 $f(x)^{-1}=f(x^{-1})$(对每个 $x\in G$)。

练习1.2.4 群的同构关系是等价关系。

群 G 到自身的同态叫作 G 的**自同态**，群 G 到自身的同构叫作**自同构**。以 $\mathrm{Aut}(G)$ 表示 G 的全体自同构所构成的集合。群 G 的两个自同构的合成仍是 G 的自同构，G 的每个自同构 f 作为一一对应的逆映射 f^{-1} 仍是 G 的自同构(这些请读者自证)。于是，$\mathrm{Aut}(G)$ 对于合成运算为群，其幺元素为 G 上的恒等自同构(即恒等映射)。对于每个群 G 决定出它的自同构群 $\mathrm{Aut}(G)$，即决定出 G 的所有自同构以及群 $\mathrm{Aut}(G)$ 的结构，是群论中的一个基本

问题。

例1.2.8 考虑整数加法群$(\mathbb{Z}, +)$。设$f: \mathbb{Z}\to\mathbb{Z}$是$\mathbb{Z}$的自同态，由练习1.2.2可知$f(0)=0$，$f(-n)=-f(n)$，从而若$f(1)=t\in\mathbb{Z}$，则$f(2)=f(1+1)=f(1)+f(1)=t+t=2t$。用数学归纳法即知，对每个自然数$n$，$f(n)=nt$，而$f(-n)=-nt$。不难看出，这是加法群$\mathbb{Z}$的自同态。因此，对于每个整数$t$，我们都可以作出$\mathbb{Z}$的自同态$f_t$：$\mathbb{Z}\to\mathbb{Z}$，$f_t(n)=nt$。不同的$t$得到不同的自同态，从而$\mathbb{Z}$的自同态集合是$\{f_t | t\in\mathbb{Z}\}$。

自同态f_t的像为$\{t_n | n\in\mathbb{Z}\}$，所以f_t是自同构的充要条件是$t=\pm 1$。于是$\mathrm{Aut}(\mathbb{Z})=\{f_1, f_{-1}\}$为二元群，其中幺元素是恒等自同构$f_1$，而$f_{-1}$是自同构$f_{-1}(n)=-n$。$\mathrm{Aut}(\mathbb{Z})$中群的运算为$f_{-1}\cdot f_{-1}=f_1$。

练习1.2.5 决定有理数加法群$\mathbb{Q}$的自同构群$\mathrm{Aut}(\mathbb{Q})$。

§1.3 子群和陪集分解

定义1.3.1 设$(G, \cdot)$是群，A为G的子集。如果$(A, \cdot)$为群，则称A为G的一个子群，表示成$A\leqslant G$。此外如果$A\neq G$，则称A是G的**真子群**，表示成$A<G$。

例如：对于每个群G，一元群$\{1_G\}$以及G自身均是G的子群，它们叫作G的**平凡子群**，G的其他子群叫作G的**非平凡子群**。

为了验证群G的子集A是G的一个子群，我们主要是验证A对于G中运算形成群，换句话说，我们需要验证以下三点：

（1）$1_G\in A$；

（2）如果$a\in A$，则$a^{-1}\in A$（即A中每个元素的逆均在A中）；

（3）$a, b\in A$，则$ab\in A$（即G中运算也是集合A中的二元运算）。至于A中运算满足结合律是显然的。因为该运算在G中已是如此。

根据这个方法，不难验证下面子群的例子。

例1.3.1 对每个整数n，$n\mathbb{Z}=\{na|a\in\mathbb{Z}\}$是整数加法群$\mathbb{Z}$的子群，并且当$n\neq 0$时这些子群均与（$\mathbb{Z}$，$+$）同构。

例1.3.2 以SL(n，$\mathbb{C}$）表示行列式为1的n阶复方阵全体，则它是一般线性群GL(n，$\mathbb{C}$）的子群。这个子群叫作**特殊线性群**。

练习1.3.1 群G的任意多个子群的交集仍是G的子群。

练习1.3.2 每个群均不能是它的两个真子群的并。

现在谈群的陪集分解。设G是群，A，B是G的子集，$a\in G$，我们今后记

$aA=\{ax|x\in A\}$，$Aa=\{xa|x\in A\}$，$A^{-1}=\{x^{-1}|x\in A\}$，$AB=\{ab|a\in A,\ b\in B\}$。

练习1.3.3 设A是群G的非空子集，则

A是G的子群$\Longleftrightarrow$如果a，$b\in A$，则$ab^{-1}\in A$

$$\Longleftrightarrow AA^{-1}\subseteq A\Longleftrightarrow A^{-1}A\subseteq A\Longleftrightarrow A^{-1}A=A。$$

引理1.3.1 设G为群，A是G的子群，定义G上的关系为：对于g，$h\in G$，$g\sim h\Longleftrightarrow gh^{-1}\in A$，则$\sim$是$G$上的等价关系，并且元素$g$所在的等价类为$Ag$。

证明

（1）对于每个元素$g\in G$，由于$gg^{-1}=1\in A$，从而$g\sim g$。

（2）如果$g\sim h$，则$gh^{-1}\in A$。由于A是子群，从而$hg^{-1}=(gh^{-1})^{-1}\in A$，因此$h\sim g$。

（3）如果$g\sim h$，$h\sim l$，则gh^{-1}，$hl^{-1}\in A$，因此$gl^{-1}=(gh^{-1})(hl^{-1})\in A$，于是$g\sim l$，综合上述即知$\sim$为$G$上的等价关系。

进而，$g\sim h\Longleftrightarrow gh^{-1}=a^{-1}\in A\Longleftrightarrow h=ag\in Ag$，从而与$g$等价的元素全体为$Ag$。证毕。

由此引理可知，群G分拆成形如Ag的一些集合的并。每个等价类Ag叫作G对于子群A的**右陪集**，如果$R=\{g_i|i\in I\}$是G对于上述等价关系的完全代表元系，则它通常叫作G对于A的

右陪集代表元系，于是有分拆

$$G=\bigcup_{g\in R}Ag(\text{非交并})$$

这叫作G对于子群A的右陪集分解。在这个分解式中右陪集的个数即是集合R的势数，表示成$[G:A]$。如果R是有限集合，则$[G:A]$是正整数$|R|$，若R为无限集合，则记成$[G:A]=\infty$。

完全类似地可以证明：

练习1.3.4 设G为群，A为G的子群，则G上的关系$g\sim h\Longleftrightarrow g^{-1}h\in A$是等价关系，并且每个等价类有形式$gA$（叫作$G$对于$A$的**左陪集**）。如果$R$是$G$对于上述等价关系的完全代表元系（叫**左陪集代表元系**），则有G对子群A的左陪集分解式 $G=\bigcup_{g\in R}gA$（非交并）。

练习1.3.5 如果R是群G对于子群A的右陪集代表元系，则R^{-1}是群G对于A的左陪集代表元系。（提示：证明$gA=hA\Longleftrightarrow Ag^{-1}=Ah^{-1}$；$a\in gA\Longleftrightarrow a^{-1}\in Ag^{-1}$。）

由练习1.3.5知，G对于子群A作右陪集分解的右陪集个数$[G:A]$也等于G对于A作左陪集分解的左陪集个数（因为$|R|=|R^{-1}|$），我们将$[G:A]$叫作子群A对于群G的**指数**。

作为陪集分解的应用，现在证明群论中第一个重要的数量结果。

定理1.3.1（拉格朗日定理） 设G为有限群，则G的每个子群A的阶均是G的阶的因子。事实上，$|G|=|A|\cdot[G:A]$。

证明 考虑G对于A的右陪集分解

$$G=\bigcup_{g\in R}Ag(\text{非交并})$$

对于A中元素a和b，由消去律可知，$a\neq b\Longleftrightarrow ag\neq bg$，所以陪集$Ag$中元素个数等于$A$中元素个数，即$|Ag|=|A|$（对每个$g\in R$）。于是由右陪集分解式即知$|G|=\sum_{g\in R}|Ag|=\sum_{g\in R}|A|=$

$|A|\cdot|R|=|A|\cdot[G:A]$。证毕。

拉格朗日定理是群论中简单而有用的定理。例如，一个6阶群只能有1，2，3，6阶的子群，不能有4阶或5阶的子群。又如：设p为素数，则一个p阶群G只能有1阶子群$\{1_G\}$和p阶子群G，即素数阶群只有平凡子群。

拉格朗日定理还有一个重要推论。设g为群G中的元素，如果存在正整数n使得$g^n=1$，则满足此式的最小正整数n叫作元素g的阶，并且称g是**有限阶元素**。例如1_G是1阶元素。如果不存在正整数n使得$g^n=1$，则称g是**无限阶元素**。注意有限群G中每个元素g均是有限阶元素，这是因为，考虑集合$\{g, g^2, g^3, \cdots\}$由于G有限，从而必有两个不同的正整数n和m，使得$g^n=g^m$。不妨设$n>m$，则$g^{n-m}=g^n\cdot(g^m)^{-1}=g^m(g^m)^{-1}=1$，而$n-m$为正整数，因此$g$是有限阶元素。

练习1.3.6 设g是群G的有限阶元素，并且阶数是n。如果对某个整数m，$g^m=1$，则必然$n|m$。(提示：应用整数的欧氏除法算式)。

定理1.3.2 设G是有限群，则G中每个元素g的阶都是G的阶$|G|$的因子。

证明 由上所述知g是有限阶元素。设g的阶是n，则$g^0=1$，g，g^2，$\cdots$，g^{n-1}是G中n个不同的元素，不难看出它形成G的一个（n阶）子群A，于是由定理1.3.1知，$|A|$(即n)是$|G|$的因子。证毕。

练习1.3.7 设G为n阶群，则对于G中每个元素g，$g^n=1$。

作为定理1.3.2的一个应用，我们决定非阿贝尔群的最小阶数。首先引入以下引理。

引理1.3.2 如果群G除了1_G之外，其余元素均是2阶的，则G是阿贝尔群。

证明 设a，$b\in G$，则$a^2=b^2=1$，$abab=(ab)^2=1$，于是$a(abab)b=ab$。但是$a(abab)b=(aa)ba(bb)=a^2bab^2=ba$，

即$ba=ab$。从而G是阿贝尔群。证毕。

引理1.3.3 素数阶群G都是阿贝尔群，并且均同构于整数模p加法群Z_p，其中$p=|G|$。

证明 由于群G的阶p是素数，根据定理1.3.2，G中每个不为1_G的元素g的阶必然是p，于是1，g，g^2，…，g^{p-1}是G中p个不同的元素，但是G中只有p个元素，从而$G=\{1, g, \cdots, g^{p-1}\}$。这显然是阿贝尔群（$g^i\cdot g^j=g^{i+j}=g^{j+i}=g^j\cdot g^i$）。由于$g^p=1$，从而易知$f: G\to Z_p, g^i\mapsto \bar{i}$是群的同构。证毕。

这个引理表明：对于每个素数p，p阶群本质上只有一个，即Z_p。

引理1.3.4 非阿贝尔群的最小阶数是6。

证明 由引理1.3.3可知2，3，5阶群均是阿贝尔群，1元群显然也是阿贝尔群。考虑4阶群G，根据定理1.3.2，G中元素$g\neq 1$的阶只能是2和4，如果G中存在4阶元素g，则$G=\{1, g, g^2, g^3\}$，它同构于Z_4，这显然是阿贝尔群。否则，G中每个元素$g\neq 1$的阶均是2。由引理1.3.2可知它也是阿贝尔群。因此，4阶群必然是阿贝尔群。最后，以S_3表示三元集合$\{1, 2, 3\}$的对称群S_3（即$\{1, 2, 3\}$的全部置换构成的群），它有$6=3!$个元素：$S_3=\{I, (12), (13), (23), (123), (132)\}$（$I$表示恒等置换）。由于$(12)(13)=(123)\neq(132)=(13)(12)$，从而$S_3$不是阿贝尔群。于是可知非阿贝尔群的最小阶数是6。证毕。

定理1.3.3 设g是群G中的n阶元素，则对于每个正整数m，g^m的阶为$n/(m, n)$。

证明 令g^m的阶数是N，由于$(g^m)^{n/(m,n)}=(g^n)^{m/(m,n)}=1$（注意$m/(m, n)$为整数），从而$N|n/(m, n)$。另一方面，由$g^{mN}=(g^m)^N=1$，可知$n|mN$。于是，$n/(m, n)|(m/(m, n)\cdot N$。但是$n/(m, n)$与$m/(m, n)$互素，因此$n/(m, n)|N$，从而$N=n/(m, n)$。证毕。

练习1.3.8 设a和b分别为群G中的n阶和m阶元素，并且$ab=ba$。求证元素ab的阶为$[n, m]$（n和m的最小公倍数）的

因子。

定理1.3.4 设G是有限群，A和B均为G的子群，则

（1）$|AB|=|B||A|/|A\cap B|$；

（2）如果$A\leqslant B\leqslant G$，则$[G:A]=[G:B][B:A]$；

（3）$[G:A\cap B]\leqslant[G:A][G:B]$，并且当$[G:A]$与$[G:B]$互素时，则$[G:A\cap B]=[G:A][G:B]$并且$AB=G$。

证明 （1）集合AB显然是一些陪集$Ab(b\in B)$的非交并，而群B是一些陪集$(A\cap B)b(b\in B)$的非交并。但是对于b，$b'\in B$，

$Ab=Ab'\Longleftrightarrow b'b^{-1}\in A\Longleftrightarrow b'b^{-1}\in A\cap B\Longleftrightarrow(A\cap B)b=(A\cap B)b'$。

所以上述两个分解中的陪集个数是一样多，即$|AB|/|A|=|B|/|A\cap B|$，从而证明了（1）。

（2）设G对B的陪集分解为$G=\bigcup\limits_{j=1}^{n}Bg_j$，$n=[G:B]$，$B$对$A$的陪集分解为$B=\bigcup\limits_{i=1}^{m}Ab_i$，$m=[B:A]$。将后式代入前式，则给出$G=\bigcup\limits_{j=1}^{n}\bigcup\limits_{i=1}^{m}Ab_ig_j$。如果$Ab_ig_j=Ab_{i'}g_{j'}$（$1\leqslant i$，$i'\leqslant m$，$1\leqslant j$，$j'\leqslant n$），则$b_{i'}g_{j'}g_j^{-1}b_i^{-1}\in A$，从而$g_{j'}g_j^{-1}\in b_{i'}^{-1}Ab_i\subseteq B$。因此$Bg_j=Bg_{j'}$，所以$j=j'$，从而$b_{i'}b_i^{-1}\in A$，即$Ab_i=Ab_{i'}$，而这又推出$i=i'$，这就证明了当$(i,j)\neq(i',j')$时，$Ab_ig_j$和$Ab_{i'}g_{j'}$是$G$对$A$的不同陪集，于是$[G:A]=mn=[G:B][B:A]$。

（3）对于b，$b'\in B$，由于$(A\cap B)b\neq(A\cap B)b'\Rightarrow b'b^{-1}\notin A\cap B\Rightarrow b'b^{-1}\notin A\Rightarrow Ab\neq Ab'$，从而可知$[B:A\cap B]\leqslant[G:A]$，所以$[G:A\cap B]=[G:B][B:A\cap B]\leqslant[G:B][G:A]$。另一方面，由上式知$[G:B]|[G:A\cap B]$。同样可证$[G:A]|[G:A\cap B]$。由假设$[G:B]$和$[G:A]$互素，所以$[G:B][G:$

$A]|[G:A\cap B]$。于是必然$[G:A\cap B]=[G:B][G:A]$，即 $\frac{|G|}{|A\cap B|}=\frac{|G|}{|B|}\cdot\frac{|G|}{|A|}$，从而$|G|=\frac{|A|\cdot|B|}{|A\cap B|}$。但是由（1）知 $|AB|=\frac{|A|\cdot|B|}{|A\cap B|}$，因此$|AB|=|G|$，即$AB=G$。证毕。

练习1.3.9 设H和K是群G的两个子群，求证G可分拆成一些双陪集$HaK(a\in G)$的非交并，并且若G是有限群，则$|HaK|=|H|\cdot[K:a^{-1}Ha\cap K]$。

练习1.3.10 设A为群G的子群，并且A在G中的指数$[G:A]$有限，则G中存在集合$\{g_1, \cdots, g_n\}(n=[G:A])$既为右陪集代表元系，也是左陪集代表元系。

定义1.3.2 设A和B是群G的两个子集，如果存在$g\in G$，使得$g^{-1}Ag=B$，则称A和B**共轭**。

不难看出，群G的子集之间的共轭关系是等价关系，每个等价类叫作是一个**共轭类**。由于$|g^{-1}Ag|=|A|$，从而彼此共轭的集合有相同的势数。此外，若A是G的子群，则易证$g^{-1}Ag$也是G的子群，叫作A的**共轭子群**。所以G的所有子群也分成一些共轭类，元素$g^{-1}ag$叫作a的**共轭元素**。

定义1.3.3 设M是群G的子集，令

$$N_G(M)=\{g\in G|g^{-1}Mg=M\}$$

这是G的一个子集，叫作M的**正规化子**。又令

$$C_G(M)=\{g\in G|g^{-1}ag=a\text{，对每个}a\in M\}$$

由于$g^{-1}ag=a$相当于$ag=ga$，从而$C_G(M)$即是与M中每个元素均可交换的G中元素全体，这也是G的一个子群，叫作M的**中心化子**。于是$C_G(G)$中元素即是与G中每个元素均可交换的那些元素，这叫作是G的**中心元素**，其全体$C(G)=C_G(G)$是G的一个子群。显然，G为阿贝尔群$\Longleftrightarrow G=C(G)$。所以群$G$的中心$C(G)$的大小反映了群$G$的交换性程度。又由定义易知$C_G(M)\leqslant N_G(M)$，而对每个元素$a\in G$，$C_G(a)=N_G(a)$。

定理1.3.5 设M是群G的子集，则与M共轭的子集个数等

于$[G:N_G(M)]$。

证明 与M共轭的子集有形式$g^{-1}Mg(g\in G)$，但是，$g^{-1}Mg=g'^{-1}Mg' \Longleftrightarrow g'g^{-1}Mgg'^{-1}=M \Longleftrightarrow gg'^{-1}\in N_G(M) \Longleftrightarrow N_G(M)g=N_G(M)g'$，从而与$M$共轭的子集个数等于$G$对$N_G(M)$的陪集个数。证毕。

系1.3.1 设a为群G中元素，则与a共轭的元素个数等于$[G:C_G(a)]$。

作为上述系理的应用，证明如下有益的结果。

定理1.3.6 设p为素数，$n\geqslant 1$，G是p^n阶群，则$|C(G)|>1$，即G有非平凡的中心元素。

证明 设$r=|C(G)|$，由于$1_G\in C(G)$，从而$r\geqslant 1$。令$C(G)=\{a_1,a_2,\cdots,a_r\}$，根据定义，元素$a$是中心元素$\Longleftrightarrow$只有$a$自身与$a$共轭，从而将$G$中分拆成共轭元素类之并时，每个中心元素$a_i(1\leqslant i\leqslant r)$均自成一类，而其余共轭类的元素个数均多于一个，$G=\{a_1\}\cup\{a_2\}\cup\cdots\cup\{a_r\}\cup A\cup B\cdots$。但是由定理1.3.5的系1.3.1可知每个共轭类的元素个数均是$p^n=|G|$的因子，所以是p的某个方幂，于是

$p^n=|G|=r+|A|+|B|+\cdots=r+p^{i_1}+p^{i_2}+\cdots$，其中$i_1,i_2,\cdots$均$\geqslant 1$，所以$r\equiv 0\pmod p$。但是$r\geqslant 1$，从而$r\geqslant p$，即存在不为幺元素的中心元素。证毕。

证明过4阶群是阿贝尔群之后，现在可以证明如下定理。

定理1.3.7 对于每个素数p，p^2阶群G均是阿贝尔群。

证明 设$a\in G$，$a\neq 1$，则a的阶为p或p^2(拉格朗日定理)。如果G中存在p^2阶元素g，则$G=\{1, g, g^2,\cdots,g^{p^2-1}\}$，这显然是阿贝尔群（同构于$Z_{p^2}$）。否则，每个元素$a\neq 1$均是$p$阶的。由定理1.3.6知，$G$中存在中心元素$a\neq 1$。而$a$的阶数是$p$，从而子群$A=\{1, a, a^2, \cdots, a^{p-1}\}$中每个元素都是中心元素。因为$|G|=p^2$，$|A|=p$，所以$G$中存在元素$b\notin A$。于是$b$的阶也为$p$，且$A$，$bA$，$b^2A$，$\cdots$，$b^{p-1}A$是$G$对$A$的$p$个陪集，并且不难证明这$p$个陪集彼此不同。因为若$b^nA=b^mA$，$0\leqslant$

$n<m\leqslant p-1$，则$b^{m-n}\in A$。但是$1\leqslant m-n\leqslant p-1$，从而$m-n$与$p$互素。所以存在整数$t$，使得$t(m-n)\equiv 1\ (\mathrm{mod}\ p)$。令$t(m-n)=1+lp$，$l\in\mathbb{Z}$，则由$b^{m-n}\in A$可知$b^{t(m-n)}\in A$，但是$b^{t(m-n)}=b^{1+lp}=b\cdot(b^p)^l=b$，这就得出$b\in A$，与假设$b\notin A$矛盾。由于$|b^iA|=|A|=p\ (0\leqslant i\leqslant p-1)$，而$|G|=p^2$，从而$G$就是$p$个陪集之并，$G=A\cup bA\cup\cdots\cup b^{p-1}A$。也就是说，$G=\{b^na^m|\ 0\leqslant n,\ m\leqslant p-1\}$，但是$a^m$为中心元素，从而$(b^na^m)(b^{n'}a^{m'})=b^n(a^mb^{n'})a^{m'}=b^n(b^{n'}a^m)a^{m'}=b^{n+n'}a^{m+m'}=(b^{n'}a^{m'})(b^na^m)$，即$G$中任意二元素均可交换，因此是阿贝尔群。证毕。

练习1.3.11 设A是有限群G的真子群，则G不能是A的全部共轭子群之并，如果A是无限群呢？

练习1.3.12 设G为群，求证对每个元素$g\in G$，映射f_g：$G\to G$，$a\mapsto g^{-1}ag$ 是群G的自同构，并且$(f_g)^{-1}=f_{g^{-1}}$。此外，f_g是恒等自同构$\Longleftrightarrow g\in C(G)$。

§1.4 循 环 群

设G是群而S是G的一个子集，G中包含S的最小子群A叫作是**由S生成的子群**，表示成$A=\langle S\rangle$。(注意：若A_1和A_2是包含S的子群，则$A_1\cap A_2$也是包含S的子群，从而包含S的子群当中确实存在最小的一个。事实上，它是G中包含S的所有子群之交。)显然，对每个元素$a\in S$，a和a^{-1}均属于$\langle S\rangle$，从而当a_1，$\cdots a_m\in S\cup S^{-1}$时，$a_1$，$\cdots$，$a_m\in\langle S\rangle$。这是这种形式的元素的逆和乘积仍旧为这种形式的元素。所以，它们形成一个子群，而这显然是包含S的最小子群。于是

$$\langle S\rangle=\{a_1\cdots a_m|\ m\geqslant 0,\ a_i\in S\cup S^{-1}\}$$

(这里当$m=0$时，理解为$a_1\cdots a_m=1$。)

如果群G自身由子集S生成，即$G=\langle S\rangle$，则称S是G的一个**生成元系**，如果G由某个有限集合S生成的，则称G是**有限生成群**。特别如果群G是由一个元素a生成：$G=\langle a\rangle$，则称G是

循环群。循环群是最简单的一类群。本节要研究这类群的性质(子群特性，生成元特性以及决定它们的自同构群)。

设$G=\langle a\rangle$是循环群。如果a是无限阶元素，则…，a^{-n}，$a^{-(n-1)}$，a^{-2}，a^{-1}，$1=a^0$，a^1，a^2，…，a^n，…是彼此不相同的元素，它们的全体即是G。因此G是无限群，并且易知$f: G\to\mathbb{Z}$，$a^n\mapsto n$是G与整数加法群$\mathbb{Z}$的同构。如果a是有限阶元素，令a的阶为$n\geqslant 1$，则$G=\{1, a, \cdots, a^{n-1}\}$与整数模$n$加法群$Z_n$同构。于是我们证明了下面的定理。

定理1.4.1 无限循环群同构于整数加法群$\mathbb{Z}$，n阶有限循环群同构于Z_n，从而同阶循环群彼此同构，而不同阶的循环群彼此不同构。

根据这个定理，n阶循环群本质上只有一个，并且当$n=\infty$时，其样板为整数加法群$\mathbb{Z}$，而当n为正整数时，其样板为整数模n加法群Z_n，它们均是阿贝尔群。由于$\mathbb{Z}$和Z_n是初等数论的研究对象，所以本节所述循环群的所有性质（及其证明），不过是初等数论中整数和同余性质的群论叙述形式。首先讨论循环群的子群。

定理1.4.2 循环群的子群都是循环群。详言之，设$G=\langle a\rangle$是循环群。

（1）如果G是无限循环群，则对于每个正整数m，G有一个指数为m的子群$G_m=\langle a^m\rangle$，并且这些和$\{1\}$是G的全部子群。

（2）如果G是n阶循环群，则对于n的每个正因子m，G有一个指数为m的子群$G_m=\langle a^m\rangle$，并且这些是G的全部子群。

证明 设H是$G=\langle a\rangle$的子群。不妨设$H\neq\{1\}$，令$m=\min\{n\mid n$为正整数，且$a^n=1\}$。由欧氏除法算式可知，若$a^l\in H$，则$m\mid l$。另一方面，若$m\mid l$，由于$a^m\in H$，显然$a^l\in H$，从而$H=\langle a^m\rangle=G_m$。当a为无限阶时，易知$[G:G_m]=m$，于是证明了（1）。如果$G=\langle a\rangle$是n阶循环群，则a的阶为n。用欧氏算法可知$m\mid n$，这是因为$n=mq+r$，$0\leqslant r\leqslant m-1$，$q\in\mathbb{Z}$。由于$a^m\in H$，从而$a^r=a^{n-mq}=(a^m)^{-q}\in H$。由于$m$的极小性，即知$r=0$，因此$m\mid n$，$n=mq$，从而$H=G_m=\langle 1, a^m, a^{2m}, \cdots,$

$a^{(q-1)m}\rangle$，这是 $q=n/m$ 阶循环群，因此 $[G:G_m]=|G|/|G_m|=n/q=m$（注意 $G_n=\{1\}$）。于是证明了（2）。证毕。

设 $G=\langle a\rangle$ 为 n 阶循环群，由拉格朗日定理知 G 的子群的阶 t 必是 n 的因子。而定理1.4.2是说：对于 n 的每个正因子 t，G 恰好有一个 t 阶子群 $\langle a^{n/t}\rangle$。

练习1.4.1 群 G 没有非平凡子群的充分必要条件是 $G=\{1\}$ 或者 G 是素数阶（循环）群。

练习1.4.2 设 G 是 n 阶有限群，如果对于 n 的每个正因子 m，G 至多只有一个 m 阶子群，则 G 为循环群。（提示：利用数论等式 $\sum\limits_{d\mid n}\varphi(d)=n$，并参考下面定理1.4.3）

定理1.4.3 设 $G=\langle a\rangle$ 是循环群。

（1）如果 G 为无限循环群，则 G 的生成元只有 a 和 a^{-1}。

（2）如果 G 为 n 阶有限群，则 G 的生成元共有 $\varphi(n)$ 个。

证明

（1）显然 $\langle a^{-1}\rangle=\langle a\rangle$，从而 a 和 a^{-1} 均是 G 的生成元。另一方面，由于 $[G:\langle a^n\rangle]=|n|$，可知 $\langle a^n\rangle=G$ 时必然 $n=\pm 1$，即 G 只有上述两个生成元。

（2）根据定理1.3.3，由于 a 的阶为 n，从而 a^m 的阶是 $n/(m,n)$，于是 $\langle a^m\rangle=G\Longleftrightarrow a^m$ 的阶是 $n\Longleftrightarrow(m,n)=1$，所以可以作为生成元的是 $a^m(1\leqslant m\leqslant n,(m,n)=1)$，而这恰好有 $\varphi(n)$ 个。

练习1.4.3 在 n 阶循环群 G 中，对于 n 的每个正因子 m，阶为 m 的元素恰好有 $\varphi(m)$ 个，由此证明等式 $\sum\limits_{m\mid n}\varphi(m)=n$。

练习1.4.4 证明：有理数加法群Q不是循环群，但是它的每个有限生成子群都是循环群。

练习1.4.5 设 a 和 b 是某个阿贝尔群 G 中的元素，阶数分别是 n 和 m，并且 $(n,m)=1$。求证 $\langle a,b\rangle$ 是 G 的 mn 阶循环子群。

练习1.4.6 设A是群G的子群，A叫作是G的**极大子群**，是指不存在G的子群B，使得$A<B<G$。

（a）决定无限循环群的全部极大子群。

（b）有限群G只有唯一的极大子群，当且仅当G是素数幂阶的循环群。

在§1.1中给出了格的定义，这里给出一个格的重要例子。群G的所有子群的集合$L(G)$，按包含关系给出序关系，即子群$H_1 \leqslant H_2$当且仅当作为集合$H_1 \subseteq H_2$，于是$L(G)$成为一个格，通常把$L(G)$叫作G的**子群格**。例如$G=Z_{24}$，它的子群格如图1-6所示。

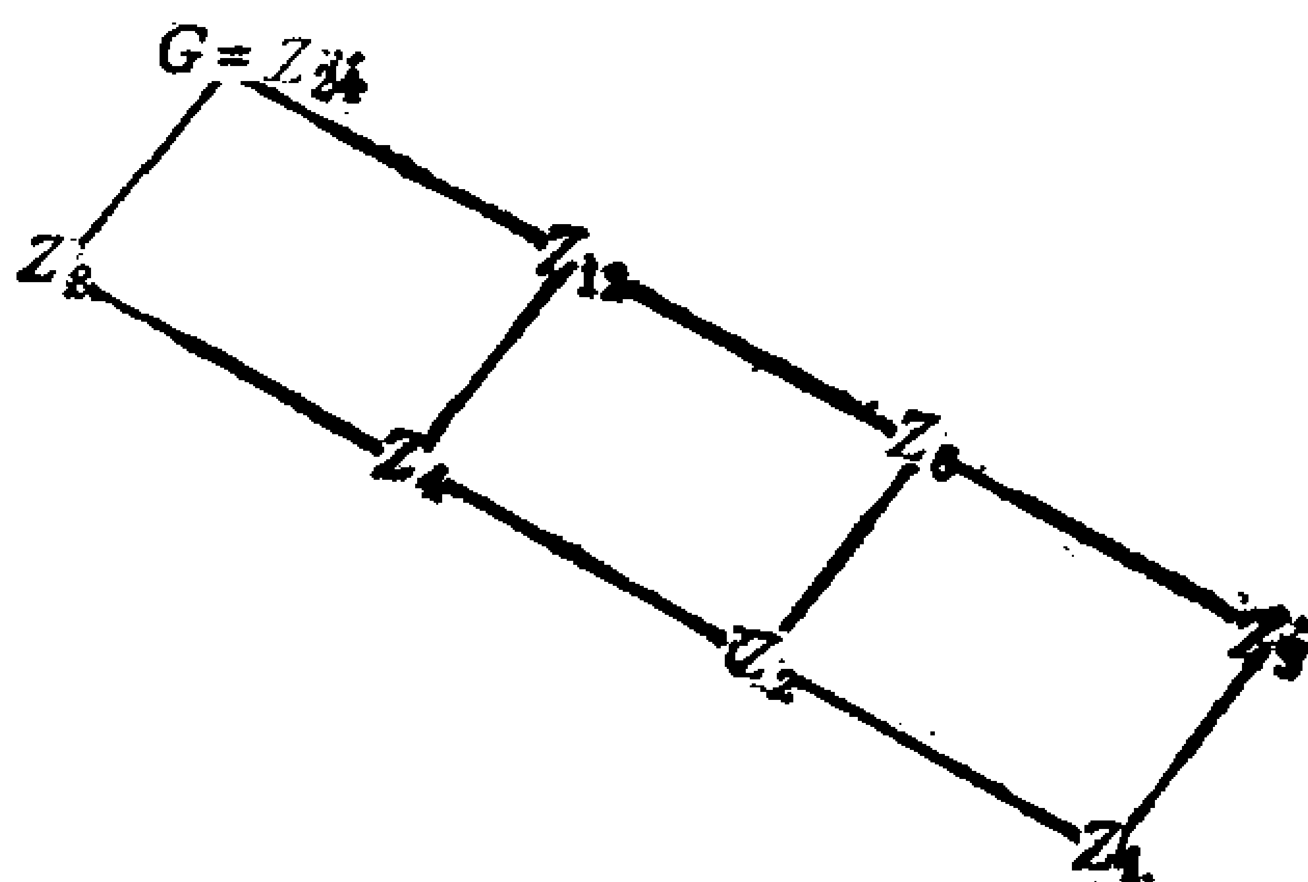


图 1-6

通常决定一个群的子群格是相当困难的，因为它意味着给出群的所有子群。在后面，将给出阶数≤15的群的子群格。

最后讨论循环群的自同构群。设$G=\langle a\rangle$是循环群，f：$G\to G$是循环群G的自同构。令$f(a)=a^m$，则$f(G)=\langle a^m\rangle$。如果f为同构，则子群$\langle a^m\rangle$等于G。从而当G为无限循环群时，必然$m=\pm 1$。可直接验证$f(a)=a$从而$f(a^m)=a^m$是恒等自同构，而$f(a)=a^{-1}$从而$f(a^m)=a^{-m}$也是同构。所以对于无限循环群G，$\mathrm{Aut}(G)$是二元群。如果$G=\langle a\rangle$是n阶有限循环群，为了$\langle a^m\rangle=G$，需要$(m, n)=1$。当这条件成立时，直接验证f_m：$G\to G$，$f_m(a^t)=a^{tm}$是群的同态，并且由上述知f_m是满同态。由于f_m将n元集合G映到n元集合G，由于f_m是满同态可知f_m也是单同态（为什么？），于是f_m是同构。从而对于n阶循环群G，

其自同构全体为 $\mathrm{Aut}(G)=\{f_m| 1\leqslant m\leqslant n, (m, n)=1\}$。由于 $f_m\cdot f_{m'}(a)=f_m(a^{m'})=f_m(a)^{m'}=a^{mm'}=f_{mm'}(a)$，于是 $f_m\cdot f_{m'}=f_{mm'}$。由此可知 $\mathrm{Aut}(G)$ 同构于整数模 n 乘法群 Z_n^*，它是 $\varphi(n)$ 阶阿贝尔群。

§1.5 正规子群 商群 同态定理

上几节已讲了不少群论中的定量结果（拉格朗日定理是典型的例子），本节主要是研究群论中的定性结果，即同态基本定理。这是研究群的最基本也是最重要的工具。为此，先讨论正规子群和商群。

设 N 是群 G 的子群，$G=\bigcup\limits_{a\in R} aN$ 是 G 对于子群 N 的陪集分解，以 $\overline{G}$ 表示全体陪集构成的集合，即 $\overline{G}=\{aN| a\in R\}$。为了将集合 $\overline{G}$ 赋以群的结构，最自然的运算是定义 $(aN)\cdot(bN)=abN$。但首先遇到的问题是如此定义运算是否可行？因为如果取 aN 和 bN 中的不同代表元 a' 和 b'，即 $aN=a'N$，$bN=b'N$ 之后，是否 $a'b'N=abN$？如果不行，那末上面的运算是不能这样定义的。

上面的讨论是相当于对 aN 和 bN 中任意元素 a' 和 b'，均应有 $a'b'N=abN$，从而要求 $aNbN=abN$。于是要求 $NbN=bN$，或者写成 $b^{-1}NbN=N$。这又相当于要求 $b^{-1}Nb\subseteq N$（对每个元素 $b\in G$）。此式又等于 $N\subseteq bNb^{-1}$。将 b 改成 b^{-1} 便得到 $N\subseteq b^{-1}Nb$（对每个 $b\in G$），从而要求 $b^{-1}Nb=N$，对每个元素 $b\in G$。换句话说，为了在 $\overline{G}$ 上能定义自然的运算，我们需要子群 N 是**自共轭**的，即只有自身是它的共轭子群。

定义1.5.1 群 G 的子群 N 叫作**正规子群**，是指对于每个元素 $g\in G$，$g^{-1}Ng=N$。如果 N 是 G 的正规子群，记成 $N\lhd G$。

引理1.5.1 设 N 是群 G 的子群，则下列条件彼此等价。

（1）$N\lhd G$；

（2）对于每个 $g\in G$，$gN=Ng$；

（3）$N_G(N)=G$；

（4）G对于N的每个左陪集均是右陪集。

证明 由于$g^{-1}Ng=N\Longleftrightarrow Ng=gN$，可知（1）和（2）等价。由于子群$N$的共轭子群的个数为$[G:N_G(N)]$，从而$N\lhd G\Longleftrightarrow N$只有一个共轭子群$\Longleftrightarrow[G:N_G(N)]=1\Longleftrightarrow G=N_G(N)$，因此（1）和（3）等价。由（2）$\Rightarrow$（4）是显然的。最后由（4）$\Rightarrow$（2），对于每个$g\in G$，由（4）可知存在$g'\in G$，使得$gN=Ng'$。由于$1\in N$，从而$g=g\cdot 1\in Ng'$，因此$Ng=Ng'=gN$。这就证明了（2）。证毕。

练习1.5.1 （a）如果$N\lhd G$，$N\leqslant M\leqslant G$，是否$N\lhd M$？

（b）如果$N\lhd M$，$M\lhd G$，是否$N\lhd G$？

设N是G的正规子群。令$\bar{a}=aN=Na$，我们可以在$\bar{G}=\{\bar{a}|a\in G\}$上定义二元运算$\bar{a}\bar{b}=\overline{ab}$。这是因为若$a'=\bar{a}$，$b'=\bar{b}$，即$a'N=aN$，$b'N=bN$，则

$$\begin{aligned}\overline{a'b'}&=a'b'N=a'b'NN=a'Nb'N=aNbN\\&=abNN=abN=\overline{ab}。\end{aligned}$$

从而上述运算与陪集代表元选取无关。不难验证集合$\bar{G}$对此运算形成群，幺元素为$\bar{1}=1\cdot N=N$，$(\bar{a})^{-1}=\overline{a^{-1}}$。我们把群$\bar{G}$叫作群$G$对于正规子群$N$的商群，表示成$\bar{G}=G/N$。如果$G$是有限群，则$|G/N|=[G:N]=|G|/|N|$。

练习1.5.2 阿贝尔群的每个子群都是正规子群。

现在讲述本节最基本的结果——同态基本定理。

定理1.5.1（**同态基本定理**） 设f：$G\rightarrow G'$是群的同态，则$\mathrm{Im}f=f(G)$是G'的子群，$\mathrm{Ker}f=\{g\in G|f(g)=1\}=f^{-1}(1)$是$G$的正规子群，并且有群的同构

$$\bar{f}:\ G/\mathrm{Ker}f\cong\mathrm{Im}f$$

这里$\cong$或者$\cong$表示群的同构，$\mathrm{Im}f$和$\mathrm{Ker}f$分别叫作同态f的像和核。

证明 先证$\mathrm{Im}f<G'$。显然$1_{G'}=f(1_G)\in\mathrm{Im}f$。如果$a',b'\in\mathrm{Im}f$，则有$a,b\in G$，使$f(a)=a'$，$f(b)=b'$。于是$(a')^{-1}=f(a)^{-1}=f(a^{-1})\in\mathrm{Im}f$，$a'b'=f(a)f(b)=f(ab)\in\mathrm{Im}f$。

这就证明 $\mathrm{Im}f$ 是G' 的子群。再证$\mathrm{Ker}f \lhd G$。不难证明 $\mathrm{Ker}f$ 是G 的子群。进而，对于每个元素$g \in G$，$a \in \mathrm{Ker}f$，$f(g^{-1}ag) = f(g^{-1})f(a)f(g) = f(g)^{-1} \cdot 1 \cdot f(g) = f(g)^{-1}f(g) = 1$，因此$g^{-1}ag \in \mathrm{Ker}f$（对每个$a \in \mathrm{Ker}f$，$g \in G$），从而 $g^{-1}(\mathrm{Ker}f)g \subseteq \mathrm{Ker}f$。类似可知$g(\mathrm{Ker}f)g^{-1} \subseteq \mathrm{Ker}f$，即 $\mathrm{Ker}f \subseteq g^{-1}(\mathrm{Ker}f)g$，于是 $g^{-1}(\mathrm{Ker}f)g = \mathrm{Ker}f$（对每个$g \in G$）。这就证明了 $\mathrm{Ker}f$是G的正规子群。最后，考虑映射

$$\bar{f}: G/\mathrm{Ker}f \to \mathrm{Im}f。$$

其中$\bar{f}$把商群$G/\mathrm{Ker}f$ 中每个元素$\bar{g} = g(\mathrm{Ker}f)$ 映成$f(g)$。首先要说明映射$\bar{f}$是可以定义的，即与$\bar{g}$的代表元素选取无关。这是因为，若$g' \in g(\mathrm{Ker}f)$，则$g' = gk$，$k \in \mathrm{Ker}f$，于是$\bar{f}(\bar{g'}) = f(g') = f(gk) = f(g)f(k) = f(g) \cdot 1 = f(g) = \bar{f}(\bar{g})$。其次，易证$\bar{f}$是群的同态，$\bar{f}(\bar{g} \cdot \overline{g'}) = \bar{f}(\overline{gg'}) = f(gg') = f(g) \times f(g') = \bar{f}(\bar{g})\bar{f}(\overline{g'})$。再证$\bar{f}$是满同态，对每个$a' \in \mathrm{Im}(f)$有$a \in G$，使$f(a) = a'$，于是$\bar{f}(\bar{a}) = f(a) = a'$。最后证明$\bar{f}$是单同态，若$\bar{a}$，$\bar{b} \in G/\mathrm{Ker}f$（$a$，$b \in G$），并且$\bar{f}(\bar{a}) = \bar{f}(\bar{b})$，则$f(a) = f(b)$，于是$f(a^{-1}b) = f(a)^{-1}f(b) = 1$，从而$a^{-1}b \in \mathrm{Ker}f$。因此$a(\mathrm{Ker}f) = b(\mathrm{Ker}f)$，即$\bar{a} = \bar{b}$。这就表明$\bar{f}$：$G/\mathrm{Ker}f \to \mathrm{Im}f$ 是群的同构。证毕。

定理中给出的$\bar{f}$叫作是**正则同构**，如果将$\bar{f}$看成是从$G/\mathrm{Ker}f$到G' 的映射（因为$\mathrm{Im}f \subseteq G'$），则$\bar{f}$是单同态，叫作**正则单同态**。

系1.5.1 设f：$G \to G'$ 是群的同态，则

（1）f为单同态$\Longleftrightarrow \mathrm{Ker}f = \{1\}$；

（2）如果f是满同态，则我们有（正则）同构$\bar{f}$：$G/\mathrm{Ker}f \cong G'$。

证明 （1）如果f为单同态，则 $\mathrm{Ker}f = f^{-1}(1_{G'})$ 只能包含一个元素1_G，即 $\mathrm{Ker}f = \{1\}$。反之，若 $\mathrm{Ker}f = \{1\}$，则当$a, b \in G$，$f(a) = f(b)$时，$f(a^{-1}b) = f(a)^{-1}f(b) = 1$，从而$a^{-1}b \in \mathrm{Ker}f$，即$a^{-1}b = 1$，于是$b = a$，因此$f$为单同态。

（2）由同态基本定理推出，因为此时 $\mathrm{Im}f=G$。

我们今后要反复使用这个同态基本定理。为了研究各种群之间的联系，我们要善于构作和发现不同群之间的同态。现在先举两个简单的例子。

例1.5.1 不难验证 $f: \mathbb{Z}\to Z_n$，$f(a)=\bar{a}$ 是加法群的满同态，并且 $\mathrm{Ker}f=n\mathbb{Z}=\{na|a\in\mathbb{Z}\}$，于是我们得到群的同构 $\mathbb{Z}/n\mathbb{Z}\simeq Z_n$。所以整数模 n 加法群 Z_n 也常常写成 $\mathbb{Z}/n\mathbb{Z}$ 的形式。

例1.5.2 det：$GL(n,\mathbb{C})\to\mathbb{C}^*$是乘法群的满同态，它把每个 n 阶可逆复方阵M映成它的行列式 $\det M$，从而行列式为 1 的 n 阶复方阵全体 $SL(n,\mathbb{C})$ 显然为 $\mathrm{Ker}f$，从而 $SL(n,\mathbb{C})\lhd GL(n,\mathbb{C})$，并且 $GL(n,\mathbb{C})/SL(n,\mathbb{C})$ 同构于$\mathbb{C}^*$（非零复数乘法解）。

定理1.5.2（第二同态定理） 设N是群G的正规子群，令$\overline{m}$为商群 $\overline{G}=G/N$ 的全部子群组成的集合，$m=\{M|N\leqslant M\leqslant G\}$（即$G$和$N$的中间群全体），则 $f: m\to\overline{m}$，$M\mapsto\overline{M}=M/N$（注意：$N\lhd M$）是一一对应。并且对于$M\in m$，$M\lhd G\Longleftrightarrow M/N\lhd G/N$。

证明 作映射 $h: \overline{m}\to m$，$\overline{M}\mapsto\{g\in G|gN=\bar{g}\in\overline{M}\}$，当 $\overline{M}\in\overline{m}$ 时，请读者证明 $h(\overline{M})=\{g\in G|\bar{g}=gN\in\overline{M}\}$是$G$的子群并且包含$N$，于是 h 是从 $\overline{m}$ 到m 的映射。由于 $fh(\overline{M})=f(\{g\in G|gN=\bar{g}\in\overline{M}\}=\overline{M})$，$hf(M)=h(\overline{M})=M$，从而 f 和 h 是互逆的映射，因此 f 是一一对应。进而，$M\lhd G\Longleftrightarrow g^{-1}Mg=M$（对每个 $g\in G$）$\Longleftrightarrow\bar{g}^{-1}\overline{M}\bar{g}=\overline{M}$（对每个 $\bar{g}\in\overline{G}$）$\Longleftrightarrow\overline{M}\lhd\overline{G}$。证毕。

练习1.5.3 利用第二同态定理给出整数加法群$\mathbb{Z}$和其子群 $n\mathbb{Z}$ 的所有中间群。

例1.5.3 我们先来决定所有的 4 元群。前面已知 4 元群G必为阿贝尔群，从而G的每个子群均是正规的。如果G中有 4 阶元素，则它同构于循环群 Z_4。否则，G中不为 1 的元素均是 2 阶的。取 $a\in G$，$a\neq 1$，则$\langle a\rangle$为G的 2 阶子群，$a^2=1$，即 $a=a^{-1}$。再取 $b\in G$，$b\neq 1, a$，则 b 也是 2 阶元素。显然 $ab\neq 1, a, b$（因为 $ab=1\Rightarrow b=a^{-1}=a$，$ab=a\Rightarrow b=1$，$ab=b\Rightarrow$

$a=1$，这均不可能)。于是 ab 就是 G 中的第四个元素，即 $G=\{1,a,b,ab\}$，其中 $a^2=b^2=1$，$ab=ba$。这个群叫作**克莱因(Klein)四元群**，记成 K_4。它显然与 Z_4 不同构，因为 Z_4 中有 4 阶元素而克莱因四元群中没有 4 阶元素。所以 4 元群本质上共有两个，K_4 和 Z_4。K_4 有三个二阶子群 $\langle a\rangle$，$\langle b\rangle$ 和 $\langle ab\rangle$，而循环群 $Z_4=\langle a\rangle$ 只有一个二阶子群 $\langle a^2\rangle$。注意商群 $K_4/\langle a\rangle$ 和 $Z_4/\langle a^2\rangle$ 均是二阶群，从而这两个商群彼此同构。这个简单的例子表明，对于 N 和 N' 分别是群 G 和 G' 的正规子群，如果 $N\cong N'$ 并且 $G/N\cong G'/N'$，我们不能推出 $G\cong G'$。

作为同态基本定理的应用，我们再给出两个同构定理。

定理1.5.3 设 $N\lhd G$，$H\leqslant G$，则 $(H\cap N)\lhd H$，$N\lhd NH\leqslant G$，并且 $NH/N\cong H/H\cap N$。

证明 由于 $N\lhd G$，从而 $NH=HN$。于是 $(NH)(NH)^{-1}=(NH)(H^{-1}N^{-1})=(NH)(HN)=N(HH)N=NHN=NNH=NH$，从而 $NH\leqslant G$。(参见练习 1.3.3) 由于 $N\lhd G$，$N\subsetneq NH\leqslant G$，因此 $N\lhd NH$。考虑映射

$$f:\ H\to NH/N,\quad h\mapsto \bar{h}=Nh。$$

易知这是群的满同态。进而对每个 $h\in H$，$h\in\mathrm{Ker}f\Longleftrightarrow f(h)=Nh=\bar{1}=N\Longleftrightarrow h\in N\Longleftrightarrow h\in H\cap N$。于是 $\mathrm{Ker}f=H\cap N$，从而 $(H\cap N)\lhd H$，并且有同构 $H/H\cap N\cong NH/N$。证毕。

定理1.5.4 设 $N\lhd G$，$M\lhd G$，$N\leqslant M$，则

$$G/M\cong\frac{G/N}{M/N}。$$

证明 设 $f:\ G/N\to G/M$，$gN\mapsto gM$。首先说明这个映射是可以定义的。如果 $gN=g'N(g,\ g'\in G)$，则 $g^{-1}g'\in N$。但是 $N\leqslant M$，从而 $g^{-1}g'\in M$，于是 $gM=g'M$，进而 f 显然是群的满同态。最后，

$gN\in\mathrm{Ker}f\Longleftrightarrow gM=M\Longleftrightarrow g\in M\Longleftrightarrow gN\in M/N$。(注意由 $N\lhd G$，$N\leqslant M$ 可知 $N\lhd M$，于是有商群 M/N。) 从而 $\mathrm{Ker}f=$

M/N，再由同态基本定理即知$\dfrac{G/N}{M/N}\cong G/M$。

练习1.5.4 $N\leqslant G$，$[G:N]=2$，求证$N\lhd G$。

练习1.5.5 若$N\lhd G$，$M\lhd G$，$M\cap N=\{1\}$。求证对于每个$a\in M$，$b\in N$，均有$ab=ba$。

练习1.5.6 （a）$C(G)\lhd G$；

（b）如果$G/C(G)$为循环群，则G是阿贝尔群；

（c）利用(2)证明，对于每个素数p，p^2阶群必是阿贝尔群。

练习1.5.7 决定S_3的全部正规子群（S_3表示$\{1,2,3\}$的全部置换组成的群）。

练习1.5.8 设G是有限阶群，$N\lhd G$，$g\in G$。如果g的阶与$|G/N|$互素，则$g\in N$。

练习1.5.9 设G为群，对每个$a\in G$，f_a：$G\to G$，$g\mapsto a^{-1}ga$是群G的自同构，叫作G的内自同构。以$I(G)$表示G的全体内自同构组成的集合。求证$I(G)\leqslant \mathrm{Aut}(G)$，并且$I(G)\cong G/C(G)$。

第二章　群在集合上的作用
西洛(Sylow)定理

除了同态基本定理之外，研究群的另一个重要的手段是群在集合上的作用，或者说成是群的置换表示。首先介绍置换群的一些知识，然后讲群的置换表示。作为它的应用，最后讲述关于群结构的深刻定理——西洛定理。

§2.1　置　换　群

设$\Sigma=\{a_1, a_2, \cdots, a_n\}$是一个$n$元集合。集合$\Sigma$到$\Sigma$的一一对应$\sigma$叫作是$\Sigma$上的一个**置换**，这个置换可以表示成

$$\sigma=\begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ \sigma(a_1) & \sigma(a_2) & \cdots & \sigma(a_n) \end{pmatrix}.$$

两个置换的乘积定义成它们作为Σ到Σ的映射的合成，即若σ和τ是Σ上两个置换，则置换$\sigma\tau$定义为$(\sigma\tau)(a_i)=\sigma(\tau(a_i))$ $(1\leqslant i\leqslant n)$。例如：

$$\begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_3 & a_2 & a_4 & a_2 \end{pmatrix}\begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_4 & a_3 & a_2 & a_1 \end{pmatrix}=\begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_2 & a_4 & a_3 & a_1 \end{pmatrix}.$$

以$S(\Sigma)$表示Σ上全部置换构成的集合，这是一个$n!$元集合。$n=|\Sigma|$，并且$S(\Sigma)$对于上述运算形成群，其幺元素是恒等置换$1_\Sigma=\begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ a_1 & a_2 & \cdots & a_n \end{pmatrix}$，置换$\begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ \sigma(a_1) & \sigma(a_2) & \cdots & \sigma(a_n) \end{pmatrix}$的逆置换是$\begin{pmatrix} \sigma(a_1) & \sigma(a_2) & \cdots & \sigma(a_n) \\ a_1 & a_2 & \cdots & a_n \end{pmatrix}$。群$S(\Sigma)$叫作**集合$\Sigma$上的对称群**，它的每个子群都叫作**集合$\Sigma$上的置换群**。设$\Sigma$和$\Sigma'$是两个

有限集合，如果$|\Sigma|=|\Sigma'|$，易知群$S(\Sigma)$和$S(\Sigma')$同构。因此，可以将n元集合上的对称群表示成S_n，而S_n的每个子群都叫作**n元集合上的置换群**。

一个置换如果将t个不同元素a_{i_1}，a_{i_2}，…，$a_{i_{t-1}}$，a_{i_t}分别映成a_{i_2}，a_{i_3}，…，a_{i_t}，a_{i_1}，把这件事写成$(a_{i_1}a_{i_2}\cdots a_{i_t})$，并且叫作是一个**轮换**，它的长度是$t$。不难看出，每个置换均可写成一些轮换的乘积，并且不同轮换没有公共的元素。例如

$$\begin{pmatrix}1&2&3&4&5&6\\1&3&2&5&6&4\end{pmatrix}=(1)(2\ \ 3)(4\ \ 5\ \ 6)。$$

长为1的轮换往往略去不写，从而上面的置换通常写为$(2\ 3)(4\ 5\ 6)$。由于不同轮换没有公共元素，所以这些轮换的前后次序可以任意改变，例如$(2\ 3)(4\ 5\ 6)=(4\ 5\ 6)(2\ 3)$。如果不计这种次序的改变，那么每个置换写成没有公共元素的一些轮换之积的方式是唯一的。

长为2的轮换叫作**对换**。例如(a_1a_2)即是把a_1和a_2分别变成a_2和a_1而其余元素不变的置换。每个轮换可以表成一些对换之积，$(a_1a_2\cdots a_n)=(a_1a_n)(a_1a_{n-1})\cdots(a_1a_2)$，所以每个置换总可以表示成有限个对换的乘积。这种表达式显然不是唯一的。但是，一个熟知的事实是，同一个置换以多种方式表示成对换之积时，其所含对换个数的奇偶性是不变的。表示成奇数个对换之积的置换叫作**奇置换**，而表示成偶数个对换之积的置换叫作**偶置换**。于是，两个奇置换之积或者两个偶置换之积必是偶置换，而一个奇置积和一个偶置换之积必是奇置换。从而若$n\geqslant 2$，并且考虑映射

$$f：S_n\to\{\pm 1\}\ \ (\{\pm 1\}是二元乘法群),$$

其中f把奇置换均映成-1，把偶置换均映成1，由上所述可知f是群的同态。当$n\geqslant 2$时，S_n中有奇置换(a_1a_2)，于是f为满同态。$\mathrm{Ker}\,f$是全体偶置换构成的集合A_n，叫作n元集合上的**交错群**。由同态基本定理知，A_n是S_n的正规子群，并且当$n\geqslant 2$时，商群S_n/A_n是二元群，从而$|A_n|=n!/2$。（注意：$S_1=A_1$，

均是一元群)。

现在研究群 S_n 和 A_n 的生成元系。

定理2.1.1 将 S_n 看成是集合 $\{1, 2, \cdots, n\}$ 上的对称群，则 (12)，(13)，…，$(1\ n)$ 是 S_n 的一个生成元系。

证明 因为每个置换均可写成有限个对换之积，并且对于 $i \neq j$，又有 $(ij)=(1i)(1j)(1i)$。

定理2.1.2 当 $n \geqslant 3$ 时，全部长为 3 的轮换形成 A_n 的一个生成元系。

证明 设 σ 是任一偶置换，并且 $\sigma \neq 1$，则 σ 是偶数个对换的乘积，所以我们只需证明任意两个对换的乘积均可用长为 3 的轮换表示即可。从而不妨设 $\sigma=(ij)(rs)$，其中 $i \neq j$，$r \neq s$。如果 $(ij)=(rs)$，则 $\sigma=1$；如果 $j=r$，$i \neq s$，则 $\sigma=(jsi)$；如果 i，j，r，s 两两不等，则 $\sigma=(ris)(ijr)$。证毕。

现在研究 S_n 的元素共轭分类。设 $\sigma \in S_n$，将 σ 写成彼此没有公共元素的轮换之积，如果其中长为 r 的轮换共有 λ_r 个$(1 \leqslant r \leqslant n)$，则称置换 σ 的型为 $1^{\lambda_1}2^{\lambda_2}\cdots n^{\lambda_n}$。显然 $\lambda_1+2\lambda_2+\cdots+n\lambda_n=n$，$\lambda_i \geqslant 0\ (1 \leqslant i \leqslant n)$。例如，$S_7$ 中的置换 $(123)(45)$ 的型为 $1^0 2^1 3^1 4^0 5^0 6^0 7^0$。当 $\lambda_i=0$ 时（即没有长为 i 的轮换时），i^{λ_i} 通常略去。例如 $(123)(45)$ 的型通常写成 $2^1 3^1$。

练习2.1.1 S_n中型为$1^{\lambda_1}2^{\lambda_2}\cdots n^{\lambda_n}$的置换共有 $n!/\prod_{i=1}^{n}(\lambda_i!(i!)^{\lambda_i})$ 个，由此证明

$$\sum_{\substack{\lambda_i \geqslant 0 \\ \lambda_1+2\lambda_2+\cdots+n\lambda_n=n}} \frac{1}{\prod_{i=1}^{n}(\lambda_i!(i!)^{\lambda_i})}=1。$$

定理2.1.3 对称群 S_n 中两个置换共轭的充分必要条件是它们有相同的型。

证明 设 σ 和 σ' 是 S_n 中的两个置换，如果 σ 和 σ' 在 S_n 中共轭，则存在 $\tau \in S_n$，使得 $\sigma'=\tau\sigma\tau^{-1}$。如果将 σ 表示成无公共

元素的轮换之积，$\sigma=(ab\cdots c)\cdots(\alpha\beta\cdots\delta)$，则$\sigma'=\tau\sigma\tau^{-1}=(\tau(a)\tau(b)\cdots\tau(c))\cdots(\tau(\alpha)\tau(\beta)\cdots\tau(\delta))$（因为$(\tau\sigma\tau^{-1})(\tau(a))=(\tau\sigma)(a)=\tau(\sigma(a))=\tau(b)$，即$\tau\sigma\tau^{-1}$把元素$\tau(a)$变成$\tau(b)$等等）。从而$\sigma'$和$\sigma$有同样的型。反之，若$\sigma$和$\sigma'$有同样的型，则由等式$\tau(ab\cdots c)\cdots(\alpha\beta\cdots\delta)\tau^{-1}=(\tau(a)\tau(b)\cdots\tau(c))\cdots(\tau(\alpha)\tau(\beta)\cdots\tau(\delta))$不难找到$\tau$，使得$\tau\sigma\tau^{-1}=\sigma'$。证毕。

以$[1^{\lambda_1}2^{\lambda_2}\cdots n^{\lambda_n}]$表示型为$1^{\lambda_1}2^{\lambda_2}\cdots n^{\lambda_n}$的全部置换组成的共轭元素类，下面是$S_4$的共轭元素类。

$[1^4]$：I（恒等置换）。

$[1^22^1]$：(12)，(13)，(14)，(23)，(24)，(34)。

$[1^13^1]$：(123)，(132)，(124)，(142)，(234)，(243)，(134)，(143)。

$[2^2]$：(12)(34)，(13)(24)，(14)(23)。

$[4^1]$：(1234)，(1243)，(1324)，(1342)，(1423)，(1432)。

练习2.1.2 证明S_4恰好有两个非平凡的正规子群。（提示：利用上述共轭元素分类和拉格朗日定理。注意：正规子群若包含某个置换，则必包含此置换所在的共轭类。）

定义2.1.1 只有平凡正规子群的群叫作**单群**。

例如：素数阶循环群只有平凡子群，从而它们均是单群。由定理1.4.2知，元素个数大于1的阿贝尔群是单群的充分必要条件是它为素数阶循环群。所以除了一元群和素数阶（循环）群之外，其他单群均是非阿贝尔群。决定全部有限非阿贝尔单群的问题具有漫长而有趣的历史，这个著名的群论问题最终于1981年才彻底解决。可是人们很早就已发现下面的定理。

定理2.1.4 当$n\geqslant 5$时，交错群A_n是单群。

证明 设$N\lhd A_n$，$N\neq\{I\}$。我们分几步证明$N=A_n$。

（1）N中必包含一个元素是长为3的轮换。事实上，设σ在N中不为恒等置换，并且σ将$\Sigma=\{a_1,\cdots,a_n\}$中尽可能多的$a_i$保持不动，我们证明$\sigma$恰好变动3个$a_i$，从而必是长为3的轮

换。首先，恰好变动两个 a_i 的置换为对换，但对换为奇置换不属于 A_n，从而 σ 变动至少 3 个 a_i，现在把 σ 写成彼此没有公共元素的一些轮换之积，并且把最长的轮换写在最左边。如果 σ 恰好变动 4 个 a_i，则 $\sigma=(a_1a_2)(a_3a_4)$。由于 $n\geqslant 5$，从而 $\beta=(a_3a_4a_5)\in A_n$，于是 $\sigma_1=\beta\sigma\beta^{-1}=(a_1a_2)(a_4a_5)\in N$。所以 $\sigma\sigma_1=(a_1a_2)(a_3a_4)(a_1a_2)(a_4a_5)=(a_3a_4)(a_4a_5)=(a_3a_4a_5)\in N$，即 N 是有长为 3 的轮换。如果 σ 变动至少 5 个 a_i，又分三种情形考虑。（a）假如 σ 包含长度 $\geqslant 4$ 的轮换，即 $\sigma=(a_1a_2a_3a_4\cdots)\cdots$，取 $\beta=(a_2a_3a_4)\in A_n$，则 $\sigma_1=\beta\sigma\beta^{-1}=(a_1a_3a_4a_2\cdots)\cdots\in N$。易知 $i\geqslant 5$ 时，$\sigma(a_i)=\sigma_1(a_i)$。从而 N 中置换 $\sigma_1\sigma^{-1}$ 至多变动 4 个 a_i，而这与 σ 变动 a_i 的个数极小性相矛盾。（b）σ 中轮换最长为 3，则 $\sigma=(a_1a_2a_3)(a_4a_5\cdots)\cdots$。由于已假定 σ 至少变动 5 个 a_i，从而 σ 不是长为 3 的轮换，于是这种形式的 σ 至少变动 6 个 a_i，取 $\beta=(a_2a_3a_4)\in A_n$，则 $\sigma_1=\beta\sigma\beta^{-1}=(a_1a_3a_4)(a_2a_5\cdots)\cdots\in N$。但是 N 中置换 $\sigma_1\sigma^{-1}$ 至多变动 5 个 a_i，又导致矛盾。（c）最后，设 σ 是一些对换之积，$\sigma=(a_1a_2)(a_3a_4)\cdots$，它至少变动 6 个 a_i，取 $\beta=(a_2a_3a_4)\in A_n$，则 $\sigma_1=\beta\sigma\beta^{-1}=(a_1a_3)(a_4a_2)\cdots\in N$，而 $\sigma\sigma_1^{-1}$ 只变动 4 个 a_i，这又导致矛盾。这就证明了 N 中包含元素是长为 3 的轮换。

（2）所有长为 3 的轮换均属于 N。因为我们在（1）中已证 N 中有长为 3 的轮换 σ。现设 σ' 是 A_n 中任意一个长为 3 的轮换，由于 σ 和 σ' 具有相同的型 3^1，从而它们在 S_n 中共轭，即有 $\tau\in S_n$，使得 $\sigma'=\tau^{-1}\sigma\tau$。如果 τ 为偶置换，即 $\tau\in A_n$，则 $\sigma'\in N$。如果 τ 为奇置换，由于 $n\geqslant 5$，而 σ 是长为 3 的轮换，从而 σ 至少固定两个文字 a_1 和 a_2，令 $\beta=(a_1a_2)$，则 $\beta\sigma=\sigma\beta$，于是 $(\beta\tau)^{-1}\sigma(\beta\tau)=\tau^{-1}\beta^{-1}\sigma\beta\tau=\tau^{-1}\beta^{-1}\beta\sigma\tau=\tau^{-1}\sigma\tau=\sigma'$。但是 $\beta\tau\in A_n$，从而 $\sigma'\in N$，这就证明 N 包含全部长为 3 的轮换。

（3）根据定理 2.1.2，全部长为 3 的轮换生成整个群 A_n，因此 $N=A_n$。这就完成了定理 2.1.4 的证明。

系2.1.1 当 $n\geqslant 5$ 时，A_n 是 S_n 的唯一非平凡正规子群。

证明 我们已讨论过$A_n \lhd S_n$。另一方面，设$N \lhd S_n$，$N \neq \{I\}$。如果$N \leqslant A_n$，则$N \lhd A_n$。根据定理2.1.4，知$N = A_n$。如果N中包含奇置换，则N中全部偶置换组成的集合$N \cap A_n$是A_n的正规子群，并且$|N \cap A_n| = \frac{1}{2}|N|$(为什么?)。于是由定理1.4知，$N \cap A_n = \{I\}$或者$A_n$。如果$N \cap A_n = A_n$，则$|N \cap A_n| = n!/2$，从而$|N| = n!$，即$N = S_n$。如果$N \cap A_n = \{I\}$，则$N$是二元群。请读者证明$S_n$不可能有二元正规子群。从而只能$N = A_n$和$S_n$，即$A_n$是$S_n$的唯一非平凡正规子群。证毕。

练习2.1.2 当$n \geqslant 3$时，$C(S_n) = \{I\}$。

练习2.1.3 求证$\mathrm{Aut}(s_3) = I(s_3) \cong s_3$。（提示：参考练习1.5.9)。

§2.2 群在集合上的作用

同态是研究群之间关系的基本手段。为了研究一个群G，自然希望有一些理想的"样板"群作为标准，然后通过研究G到样板群的各种同态来把握G的特性。理想的样板群有两类，一类是置换群，另一类是矩阵群。一个群G到置换群的同态叫G的**置换表示**，到矩阵群的同态叫**线性表示**。研究群的线性表示是群论的一个重要分支，即通常所谓**群表示理论**。它在物理，化学，力学等许多方面都得到重要应用。本节的目的是介绍群的置换表示理论的一些基本知识。

设Σ是一个集合，$S(\Sigma)$是Σ上的对称群。群G到$S(\Sigma)$的每个同态$f: G \to S(\Sigma)$都叫作群G在集合Σ上的一个**置换表示**。如果f是单同态，则称f是**忠实表示**。这时，对于G中不同的元素g，$f(g)$是Σ上不同的置换。群G借助于置换表示f作用在集合Σ之上，也就是说，元素$g \in G$在集合Σ上的作用看成是置换$f(g)$，对于每个$a \in \Sigma$，定义$ga = f(g)(a)$。

设$\pi: G \to S(\Sigma)$是一个置换表示。在Σ上定义如下的关系：对于$a, b \in \Sigma$，

$$a \sim b \Longleftrightarrow \text{有 } g \in G, \text{ 使得 } ga = b.$$

这是一个等价关系，因为

（1）$\pi(1_G)$ 是Σ的恒等置换，从而对每个$a\in\Sigma$，$1_Ga=a$，即$a\sim a$；

（2）如果$a\sim b$，则有$g\in G$，使$ga=b$。于是$g^{-1}b=a$，即$b\sim a$；

（3）若$a\sim b$，$b\sim c$，则$ga=b$，$hb=c$，其中g，$h\in G$。于是$(hg)a=c$，所以$a\sim c$（简言之，$\sim$是等价关系，因为G是群）。

对于上述等价关系，Σ中元素a所在的等价类是$[a]=Ga=\{ga|g\in G\}$，每个等价类叫一个**G-轨道**，或简称**轨道**。于是集合Σ分拆成一些轨道。在同一轨道中，可以通过某个$g\in G$的作用将其一个元素变成另一个元素，但不同轨道中的两个元素不可以这样作。如果G在Σ上的作用只有一个轨道，则称G在Σ上是**传递的**。显然，如果将G看成它在某一个G-轨道上的作用，则G显然是传递的。

例2.2.1 设G是群，取$\Sigma=G$。如下作映射：

$\rho: G\to S(G)$，$\rho(g)a=ga$（对每个g，$a\in G$）。也就是说，对于$g\in G$，$\rho(g)$是集合G上如下的置换：它将G的每个元素a变成ga（由群G上的消去律可知$\rho(g)$是G上的置换），由于

$$(\rho(g)\rho(g'))a=\rho(g)(\rho(g')a)=\rho(g)(g'a)$$
$$=gg'a=\rho(gg')a,$$

从而$\rho(g)\rho(g')=\rho(gg')$，即$\rho: G\to S(G)$是群的同态，即$\rho$是群$G$在集合$G$上的一个置换表示，这叫作群$G$的**左正则表示。**由于

$$g\in \mathrm{Ker}\,\rho\Longleftrightarrow ga=a\ (对每个a\in G)\Longleftrightarrow g=1_G$$

于是ρ为单同态，即左正则表示是忠实的。

类似地定义

$$\tau: G\to S(\Sigma),\quad \tau(g)a=ag^{-1},$$

则 $$(\tau(g)\tau(g'))a=\tau(g)(ag'^{-1})=ag'^{-1}g^{-1}$$

$$= a(gg')^{-1} = \tau(gg')a。$$

可知τ也是一个群同态。表示τ叫作G的**右正则表示**，它也是忠实的。

作为正则表示的应用，有如下定理。

定理2.2.1 凯莱（Cayley）定理 每个群均同构于某个置换群。

证明 由于正则表示ρ（或者τ）：$G\to S(G)$是忠实的，根据同态基本定理，G同构于$\rho(G)$，因为$\rho(G)$是集合G上对称群$S(G)$的子群，从而$\rho(G)$是集合G上的置换群。证毕。

这个定理充分显示出置换群可以作为样板群，但是一般来讲，集合G太大。我们希望能给出群G在较小集合Σ上的置换表示，因为$n=|\Sigma|$愈小，$S(\Sigma)=S_n$的子群愈容易研究。

例2.2.2 设$H\leqslant G$，取$\Sigma=\{aH|a\in G\}$，即Σ是G对于H的全部陪集aH构成的集合。定义

$$\rho_H: G\to S(\Sigma),\ \rho_H(g)(aH)=gaH$$

即对每个$g\in G$，$\rho_H(g)$把陪集aH变成gaH。这是集合H上的置换，并且ρ_H是群的同态，从而ρ_H给出G的一个置换表示，叫作群G对于子群H的**左诱导表示**。由于

$$g\in\rho_H\Longleftrightarrow gaH=aH(\text{对每个 }a\in G)\Longleftrightarrow a^{-1}ga\in H(\text{对每个 }a\in G)\Longleftrightarrow g\in aHa^{-1}(\text{对每个}a\in G)\Longleftrightarrow g\in\bigcap_{a\in G}aHa^{-1},$$
从而

$$\mathrm{Ker}\,\rho_H=\bigcap_{a\in G}aHa^{-1}(\text{即}H\text{的所有共轭子群之交})。$$

类似可定义G对于子群H的**右诱导表示**：$\Sigma=\{Ha|a\in G\}$，τ_H：$G\to S(\Sigma)$，$\tau_H(g)(Ha)=Hag^{-1}$，$\mathrm{Ker}\tau_H$也是H的所有共轭子群之交。

例2.2.3 设A是群G的任意子集，取$\Sigma=\{aAa^{-1}|a\in G\}$（即$A$的全部共轭子集）。定义

$$\pi: G\to S(\Sigma),\ \pi(g)(aAa^{-1})=gaAa^{-1}g^{-1}=(ga)A(ga)^{-1},$$

这是一个置换表示，叫作群G对于子集A的**共轭表示**。由于

$$g \in \operatorname{Ker}\pi \Longleftrightarrow gaAa^{-1}g^{-1}=aAa^{-1}(\text{对每个 } a \in G) \Longleftrightarrow$$
$$g \in N_G(aAa^{-1})=aN_G(A)a^{-1}(\text{对每个 } a \in G)$$

从而 $\operatorname{Ker}\pi = \bigcap\limits_{a \in G} aN_G(A)a^{-1}$，即为正规化子群 $N_G(A)$ 的所有共轭子群之交。

设群G作用于集合Σ之上，则对每个元素$a \in \Sigma$. $G_a=\{g \in G \mid ga=a\}$是$G$的一个子群，叫作元素$a$的**固定子群**。

练习2.2.1 设a，$b \in \Sigma$，$ga=b\,(g \in G)$，则$G_a=g^{-1} \times G_b g$，换句话说，同轨道中元素的固定子群彼此共轭。

定理2.2.2（轨道公式） 设有限群G作用于集合Σ上，$a \in \Sigma$，则$|G|=|G_a|\cdot|[a]|$。

证明 作G对子群G_a的陪集分解

$$G=g_1G_a \cup g_2G_a \cup \cdots \cup g_nG_a, \quad n=[G:G_a]。$$

令$g_ia=a_i\,(1 \leqslant i \leqslant n)$，对于每个$g \in G$，则有唯一的$i\,(1 \leqslant i \leqslant n)$使得$g \in g_iG_a$。令$g=g_ih$，$h \in G_a$，则$ga=(g_ih)a=g_ia=a_i$。但是

$$a_i=a_j \Longleftrightarrow g_ia=g_ja \Longleftrightarrow g_j^{-1}g_ia=g_j^{-1}g_ja=1_Ga=a$$
$$\Longleftrightarrow g_j^{-1}g_i \in G_a \Longleftrightarrow g_iG_a=g_jG_a \Longleftrightarrow i=j,$$

从而a_1，…，a_n两两相异，于是$[a]=\{a_1, a_2, \cdots, a_n\}$是$n$元集合，即$|[a]|=n=[G:G_a]=|G|/|G_a|$。证毕。

系2.2.1 设有限群G作用在有限集Σ上是传递的，则对于每个$a \in \Sigma$，$|G|=|G_a|\cdot|\Sigma|$。

注意 （1）当G是无限群时，如果$[G:G_a]$有限，则$[a]=[G:G_a]$也是正确的。证明同上。

（2）利用例2.2.3的共轭表示和定理2.2.2，又得到第一章所证的：设A为群G的子集，则A的共轭子集个数$=[G:N_G(A)]$。

练习2.2.2 设群G在集合Σ上的作用是传递的，$N \lhd G$，则Σ在群N的作用下每个N-轨道都包含同样多的元素。

练习2.2.3 设有限群G作用在有限集合Σ上，以t表示Σ的G-轨道个数，对于每个$g \in G$，以$f(g)$表示Σ在g作用下

的不动元素个数，即 $f(g)$ 等于 $\{a\in\Sigma \mid ga=a\}$ 的势数。求证 $\sum\limits_{g\in G} f(g)=t|G|$，换句话说，$G$ 的每个元素"平均"将 Σ 中 t 个元素保持不动。

例2.2.4 正 n 边形的对称群（$n\geqslant 3$）。 设正 n 边形的顶点依次为 1，2，…，n（如图 2-1 所示)。通过平面上欧氏运动和反转将正 n 边形变成自身的每个运动叫作是该正 n 边形的一个**对称**。全体这种对称自然形成一个群，叫作**正 n 边形的对称群**，表示成 D_n。我们来决定这个群。

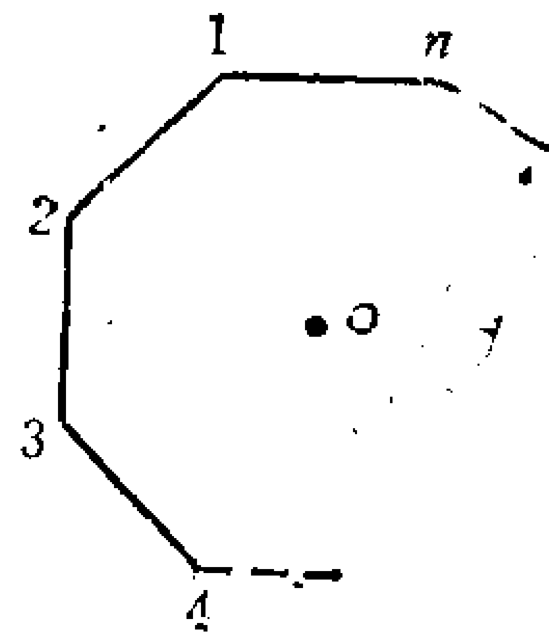


图 2-1

D_n 中的元素显然是正 n 边形 n 个顶点的一个置换，并且它由这个置换所完全决定，所以我们可以把 D_n 看成是 n 个顶点 $\{1, 2, \cdots, n\}$ 上的置换群。首先，绕正 n 边形中心 o 反时针旋转 $\frac{2\pi}{n}$ 角度的旋转是 D_n 中的元素，它看成顶点置换则为 $\sigma=(123\cdots n)$，这是 n 阶元素。由于 $\sigma^i(1)=i+1$（$\delta\leqslant i\leqslant n-1$），所以 D_n 在 $\{1, 2, \cdots, n\}$ 上的作用是传递的。其次，将顶点 1 固定的对称一共有两个，除了恒等置换之外还有将顶点 1 不动的反射：

$$\tau=\begin{cases}(2n)(3\ n-1)\cdots\left(\frac{n}{2}\quad \frac{n}{2}+2\right), & \text{如果 } 2\mid n\\ (2n)(3\ n-1)\cdots\left(\frac{n+1}{2}\quad \frac{n+3}{2}\right), & \text{如果 } 2\nmid n\end{cases}$$

从而顶点 1 的固定子群是 2 阶的。根据轨道公式便知 $|D_n|=2n$（系 2.2.1)。注意 τ 是 2 阶元素，并且容易验证 $\sigma^i\tau^j$（$0\leqslant i\leqslant n-1$，$0\leqslant j\leqslant 1$）是 $2n$ 个不同的对称，从而它们给出群 D_n 的全部元素。这个群的运算法则由 $\sigma^n=1$，$\tau^2=1$ 和 $\tau\sigma=\sigma^{-1}\tau$ 所完全决定。

最后用群在集合中的作用解决一些群论问题。

引理2.2.1 设G是$2n$阶群，$2\nmid n$，则G必有指数为2的正规子群。

证明 考虑G的左正则表示$\rho:G\to S(G)=S_{2n}$，由于ρ是忠实表示，因此$G\cong\rho(G)$，于是只需对置换群$\rho(G)$证明引理即可。注意群G中必有2阶元素g（证明：将G中每个元素a和a^{-1}放在一组，如果$a^2\neq 1$，即$a\neq a^{-1}$，则组$\{a, a^{-1}\}$包含两个元素，但是$1^{-1}=1$，从而组$\{1, 1\}$只含一个元素。由于G有偶数个元素，从而至少还有一组$\{g, g^{-1}\}$也只含一个元素，即g的阶为2）。由于$g^2=1$，$g\neq 1$，从而$\rho(g)a\neq a$，$\rho(g)^2a=a$（对每个$a\in G$），因此置换$\rho(g)$是一些对换$(a\ \rho(g)a)$之积。由于G共有$2n$个元素，从而$\rho(g)$是n个对换之积。由假设n为奇数，从而$\rho(g)$为奇置换。总之，已证明了解$\rho(G)$中包含奇置换，从而$\rho(G)$中共有一半是偶置换，它们构成$\rho(G)$的指数为2的子群，而指数为2的子群必是正规的。证毕。

由此得到下面的重要定理。

定理2.2.3 设G为有限群，并且$|G|\geqslant 6$，$|G|\equiv 2 \pmod 4$，则G不是单群。

引理2.2.2 设G为有限群，p是$|G|$的最小素因子，如果$N\leqslant G$，$[G:N]=p$，则$N\lhd G$。

证明 考虑G对于子群N的诱导表示：

$$\rho_H:\ G\to S_p,\ \operatorname{Ker}\rho_H=\bigcap_{a\in G}a^{-1}Na\leqslant N.$$

从而$p=\dfrac{|G|}{|N|}$除尽$|G|/|\operatorname{Ker}\rho_H|$，由于$p^2\nmid p!=|S_p|$，而$G/\operatorname{Ker}\rho_H$同构于$S_p$的一个子群，从而$p^2$除不尽$|G/\operatorname{Ker}\rho_H|$。另一方面$|G/\operatorname{Ker}\rho_H|$没有比$p$大的素因子，由对$p$的假设可知它也没有比$p$小的素因子，从而$|G\backslash\operatorname{Ker}\rho_H|=p$，但是$[G:N]=p$，并且$\operatorname{Ker}\rho_H\leqslant N$，从而$\bigcap\limits_{a\in G}a^{-1}Na=\operatorname{Ker}\rho_H=N$，即$a^{-1}Na=N$（对

每个$a\in G$)，于是$N\lhd G$。证毕。

练习2.2.4 设p为素数，G为p^n阶群（$n\geqslant 1$），求证G的非正规子群的个数是p的倍数。(提示：设Σ是G的全部子群组成的集合，考虑G在Σ上的共轭作用。)

练习2.2.5 设G是一个单群，如果存在G的真子群H使得$[G:H]\leqslant 4$，则$|G|\leqslant 3$。（提示：令$n=[G:H]$，考虑G对于H的诱导表示$\rho=\rho_H$: $G\to S_n$, $\rho(g)aH=gaH$。$\mathrm{Ker}\,\rho=\bigcap aHa^{-1}$是$G$的正规子群，并且$\mathrm{Ker}\,\rho\leqslant H$。由于$H$为$G$的真子群，从而$\mathrm{Ker}\,\rho$为$G$的真正规子群。但是$G$为单群，于是$\mathrm{Ker}\,\rho=\{1\}$，即$\rho$为单同态，从而$G\cong\rho(G)\leqslant S_n$，而$2\leqslant n\leqslant 4$。再考查$S_n(2\leqslant n\leqslant 4)$中子群为单群的阶均$\leqslant 3$，即证。)

练习2.2.6 设有限群G的阶数为$2^n m$，m为奇数$n\geqslant 1$。如果G含有2^n阶元素，则G有指数为2^n的正规子群（特别地，G不是单群)。（提示：只需证明G有指数为2的（正规）子群，因为由此利用定理1.5.2转到商群后对n归纳即可证得原命题。考虑G的左正则表示ρ: $G\to S_{2^n m}$, $\rho(g)g'=gg'$，这是忠实表示，从而只需证$\rho(G)$有指数2的子群。设a为G中2^n阶元素，则$\rho(a)$是m个轮换之积，每个轮换长为2^n，从而$\rho(a)$是奇置换。于是$\rho(G)$中全体偶置换即为所求。)

练习2.2.7 设G为无限群，如果G有指数有限的真子群。求证G必有指数有限的真正规子群。（提示：设H是G的指数有限的真子群，$n=[G:H]\geqslant 2$。考虑G在n个陪集$\{g_1H,\cdots,g_nH\}$上的左乘作用τ: $G\to S_n$, $\tau(g)g_iH=gg_iH$，则$M=$

$$\mathrm{Ker}\,\tau=\bigcap_{i=1}^{n}g_iHg_i^{-1}\lhd G,$$

由于$G/M\cong\tau(G)$，而$\tau(G)$为有限群S_n的子群，从而$[G:M]=|\tau(G)|$有限，并且$M\leqslant H<G$，所以M是G的真子群。)

§2.3 西洛定理

拉格朗日定理是说：若有限群G的阶数是n，则G的每个子群的阶都是n的因子。反过来，对于n的每个因子d，G未必有d阶子群。例如我们已知60阶群A_5是单群，它没有30阶子群，因为这样的子群一定是正规的。但是下一定理表明，对于$|G|$的特殊的因子d，G必有d阶子群。在本定理以及以后许多结果的证明中，将不断使用群在集合上作用这一有效工具。

定理2.3.1 设$p^r\|\,|G|$，其中p为素数。以$N(n)$表示G中n阶子群的个数，则$N(p^r)\equiv 1 \pmod p$。特别地，如果$p^r\|\,|G|$，则G至少存在一个p^r阶子群。

证明 令$|G|=p^rn$。以Σ表示G的全部p^r元子集组成的集族，则$|\Sigma|=C_{p^rn}^{p^r}$。考虑G在Σ上的如下作用：

ρ：$G\to S(\Sigma)$，$\rho(g)M=Mg^{-1}$(对于$g\in G$，$M\in\Sigma$)。则Σ分拆成一些轨道T_i之并：

$$\Sigma=\bigcup_i T_i,\ \ |\Sigma|=\sum_i|T_i|,\ \ |T_i|=[G:A_i],$$

其中$A_i=\{g\in G|M_ig=M_i\}$是轨道T_i中任一元素M_i的固定子群。由于$M_iA_i=M_i$，从而M_i可分拆成：

$$M_i=\bigcup_{j=1}^{k_i} g_{ij}A_i,\ \ g_{ij}\in M_i(1\leqslant j\leqslant k_i),$$

$k_i=|M_i|/|A_i|=p^r/|A_i|$，于是$|A_i|=p^{r_i}$，$r_i\leqslant r$。

如果$r_i<r$，则$|T_i|=[G:A_i]=np^{r-r_i}\equiv 0 \pmod{pn}$。如果$r_i=r$，则$|T_i|=n$。于是

$$C_{np^r}^{p^r}=|\Sigma|=\sum_i|T_i|\equiv\sum_{|T_i|=n}|T_i|=n\cdot\sum_{|T_i|=n}1 \pmod{pn}.$$

现在计算$\sum\limits_{|T_i|=n}1$（即长为n的轨道T_i的个数）。注意：$|T_i|=n$ $\Rightarrow|A_i|=p^r\Rightarrow k_i=1\Rightarrow M_i=g_iA_i$，于是$p^r$阶子群$B_i=g_iA_ig_i^{-1}$与$M_i$

$=g_iA_i$ 在同一轨道T_i之中，并且若$X\in T_i$，则 $Xg=M_i=B_ig_i$，于是$X=B_ig_ig^{-1}$，所以轨道 T_i 中 n 个元素即是G对于 p^r 阶子群B_i的 n 个陪集。注意这 n 个陪集之中除 B_i 外其余陪集不包含 1，从而不会是子群。这就表明，G的每个p^r 阶子群均恰好在一个长为 n 的轨道之中。于是 $\sum_{|T_i|=n} 1=N(p^r)$，从而

$$C_{np^r}^{p^r}\equiv nN(p^r)\pmod{pn}。$$

这个同余式对于任意满足定理条件的G均对。特别取G为 p^rn 阶循环群，则它只有一个 p^r 阶子群。代入上式即知 $C_{np^r}^{p^r}\equiv n\pmod{pn}$，于是

$n\equiv nN(p^r)\pmod{pn}$，从而$N(p^r)\equiv 1\pmod{p}$。证毕。

定义2.3.1 设 G 为 p^rn 阶群，其中 p 为素数，$r\geqslant 1$，$p\nmid n$，则G的每个 p^r 阶子群均叫作G的西洛 p-子群。

定理2.3.2 西洛定理 设G为有限群，

（1）对于$|G|$的每个素因子 p，G均存在西洛 p-子群。

（2）G的西洛 p-子群彼此共轭。

（3）G的西洛 p-子群个数$\equiv 1\pmod{p}$。

（4）设P是G的一个西洛 p-子群，则G的西洛 p-子群个数为$[G:N_G(P)]$。

证明 （1）和（3）由定理1直接推出，由（2）容易得到（4），从而只需证（2）。令Σ是G的所有西洛 p-子群构成的集合，将G共轭作用于其上。令$\triangle$是一个G-轨道，取$P\in\Sigma$，再将P共轭作用于$\triangle$上（由于G中元的作用是$\triangle$上的置换，从而P中元也是如此），于是$\triangle$分拆成一些P-轨道，每个P-轨道的长度是$|P|=p^r$的因子。如果$P'\in\triangle$，并且 P' 自身组成一个P-轨道，即 $xP'x^{-1}=P'$（对每个$x\in P$），则$P\leqslant N_G(P')$，从而$PP'\leqslant G$。但是$|PP'|=|P||P'|/|P\cap P'|$仍为 p 的幂，并且$P\leqslant PP'$，由于P和 P' 均是西洛P-群，从而必然$P=PP'=P'$。这就表明：当$P\in\triangle$时，$\triangle$中长为 1 的轨道只有$\{P\}$，从而$|\varDelta|\equiv 1\pmod{p}$，而$P\notin\varDelta$时，$\varDelta$没有长为 1 的轨道，从而$|\varDelta|\equiv 0$

$(\bmod p)$。但是这两种情形不可能同时发生，所以只能是所有西洛 p-子群均在 Δ 中，即 $\Sigma=\Delta$。换句话说，G 在 Σ 上的共轭作用是传递的，即 G 的所有西洛 p-子群彼此共轭。证毕。

系2.3.1 设素数 p 是 $|G|$ 的因子，则群 G 的每个 p 方幂阶的子群 B 均包含在 G 的某个西洛 p-子群之中。

证明 仍以 Σ 表示 G 的全部西洛 p-群，由定理2.3.2可知 $|\Sigma|\equiv 1 \pmod p$。将 B 共轭作用于 Σ 上，每个 B-轨道的长度是 $|B|$ 的因子，从而为 p 的方幂。由 $|\Sigma|\equiv 1 \pmod p$ 可知必然有长为 1 的 B-轨道 $\{P\}$。与证明定理2.3.2的（2）一样可由此推出 $BP=P$，于是 $B\leqslant P$，即 B 包含在西洛 p-子群 P 之中。证毕。

系2.3.2 设 P 是 G 的西洛 p-子群，$A\leqslant G$，并且 $N_G(P)\leqslant A$，则 $N_G(A)=A$。

证明 只需证 $N_G(A)\leqslant A$。设 $g\in N_G(A)$，则 $g^{-1}Ag=A$，从而 $g^{-1}Pg\leqslant g^{-1}Ag=A$。由于 $P\leqslant N_G(P)\leqslant A\leqslant G$，从而 P 为 A 的西洛 P-子群。由于 $g^{-1}Pg\leqslant A$ 而 $|P|=|g^{-1}Pg|$，从而 $g^{-1}Pg$ 也是 A 的西洛 p-子群。由定理 2 即知存在 $a\in A$，使得 $a^{-1}(g^{-1}pg)a=P$，即 $ga\in N_G(p)\leqslant A$，于是 $g\in A$。证毕。

系2.3.3 $M\lhd G$。P 为 M 的西洛 p-子群，则 $G=MN_G(p)$。

证明 对每个 $g\in G$，$g^{-1}Pg\leqslant g^{-1}Mg=M$。于是，由定理2.3.2知有 $k\in M$ 使得 $k^{-1}(g^{-1}Pg)k=P$，即 $gk\in N_G(p)$，从而 $g=(gk)k^{-1}\in N_G(P)M=MN_G(P)$。证毕。

练习2.3.1（凯莱） 若 p 是 $|G|$ 的素因子，则有限群 G 必有 p 阶元素。

练习2.3.2 若 p 是 $|G|$ 的素因子，则方程 $x^p=1$ 在 G 中的解数 $\equiv 0 \pmod p$。

现在我们举几个具体的例子。

例2.3.1 148阶群不是单群。

证明 取 $p=37|148$，则 $N(37)\equiv1(\bmod 37)$，从而 $N(37)=37l+1$。由于148阶群 G 的全部西洛37-子群形成一个共轭类，故

其总数应当是$|G|=148$的因子，即$N(37)=37l+1|148$，于是$37l|4$这只能$l=0$，即$N(37)$。因此，G只有一个37阶子群，从而必然是正规子群（定理2.3.2的（2）），因此G不是单群。

例2.3.2 56阶群G不是单群。

证明 与前例一样，$N(7)=7n+1|56$，从而$7n+1|8$，于是$N(7)=1$或8。如果$N(7)=1$，则7阶西洛子群是正规的。如果$N(7)=8$，令P_1，…，P_8是G的8个不同的7阶子群，则任意两个只有公共元素1，从而合起来共占了$6\times8+1=49$个元素，余下$56-49=7$个元素加上1_G必然形成G的8阶西洛2-子群，从而G的8阶西洛子群只有一个。于是为正规子群，所以G不是单群。

练习2.3.3 200阶群G不是单群。

练习2.3.4 求证最小的非阿贝尔群必同构于S_3。

练习2.3.5 设G为有限群，$N\lhd G$，p和$|G/N|$互素，则N包含G的所有西洛p-子群。

定理2.3.3 设p和q是两个素数，则pq阶群G必不是单群。

证明 若$p=q$，已证p^2阶群G是阿贝尔群，由定理2.3.1知它有p阶子群，而阿贝尔群的子群都是正规的，从而G不是单群。如果$p\neq q$，不妨设$p>q$，则$N(p)=np+1|q$，而$q<p$，从而只能$n=0$，即G只有一个p阶西洛子群，它是正规子群。于是G也不是单群，证毕。

定理2.3.4 设p和q是素数，则p^2q阶群G不是单群。

证明 若$p=q$，已证过p^3阶群G必有非平凡的中心$C(G)$，于是$C(G)$必有p阶子群N，显然$N\lhd G$，从而G不是单群。

如果$p>q$，则$N(p^2)=np+1|q$，$q<p$，于是$n=0$。从而G有正规的p^2阶西洛子群，于是G不为单群。

最后设$p<q$，则$N(q)=nq+1|p^2$。如果$nq+1=1$，则G有正规q阶子群，即不是单群。由于$p<q$，从而$nq+1$不能为p。最后若$N(q)=nq+1=p^2$，即G有p^2个q阶子群，它们共占据了G的$p^2(q-1)+1$个元素。余下p^2-1个元素和1_G便组成

G的唯一的 p^2 阶西洛子群P，于是$P\lhd G$，所以G也不为单群。证毕。

证明如下定理作为本章的结束。

定理2.3.5 非阿贝尔单群的最小阶数是60，并且60阶单群必同构于A_5。

证明 到目前为止我们已证明了下列诸结果：

p^n（$n\geqslant 2$，p为素数）阶群有非平凡的中心，从而不是单群；

pq阶群，p^2q阶群（p和q为素数）均不是单群；

$2m$（m为奇数，$m\geqslant 3$）阶群不单；

素阶循环群已在定理2.3.5考虑之外，故不讨论。在59之内除了上述情形之后只剩下$|G|=24,36,40,48,56$。例2.3.2表明56阶群不单；40阶群有唯一的5阶西洛子群，从而不单；

设$|G|=48=3\times 16$，则易知G的16阶西洛子群的个数为1或3（$N(16)=2n+1\mid 3$，所以$N(16)=1$或3）。若$N(16)=1$则G不单。若$N(16)=3$，令P_1，P_2，P_3为G的3个16阶西洛子群，G在$\{P_1, P_2, P_3\}$上的共轭作用给出同态ρ：$G\to S_3$。令$N=\mathrm{Ker}\rho$，则$N\lhd G$。由于$|G|=48>|S_3|=6$，从而$N\neq\{1\}$。又由于P_1，P_2，P_3彼此共轭，从而$N\neq G$，于是N是G的非平凡正规子群，故48阶群不单。类似地可证36阶群不单。

设$|G|=24=3\times 8$，则3阶西洛群的个数为1或4。若$N(3)=1$，则G不单。若$N(3)=4$，令P_1，P_2，P_3，P_4为G的4个3阶西洛子群。考虑G在$\{P_1, P_2, P_3, P_4\}$上的共轭作用给出同态ρ：$G\to S_4$，由于P_i（$1\leqslant i\leqslant 4$）彼此共轭，因此$\mathrm{Ker}\rho\neq G$。如果$\mathrm{Ker}\rho=\{1\}$，则ρ为单同态。但是$|G|=|S_4|=24$，从而$G\cong S_4$。可是S_4不为单群，所以G不单。如果$\mathrm{Ker}\rho\neq\{1\}$，则$\mathrm{Ker}\rho$为$G$的非平凡正规子群，从而$G$也不单。

最后考虑$|G|=60$。已证过A_5为单群。现在我们证明60阶单群G必然同构于A_5。先证明G有指数为5（即12阶）的子群。为此，令P是G的一个4阶西洛子群，从而$N(4)=[G:N_G(P)]$，

由G为单群可知$[G:N_G(P)]=N(4)\neq 1$。又由练习2.2.5知，$[G:N_G(P)]\neq 2$，3，4，从而$4\leqslant|N_G(P)|<15$。由$P\leqslant N_G(P)\leqslant G$可知，$4\,||N_G(P)||\,60$。如果$|N_G(P)|\neq 12$，则必然$|N_G(P)|=4$，于是$G$有15个4阶西洛子群。如果它们两两只有公共元素$1_G$，则它们共占去$G$的$15\cdot 3+1=46$个元素。由于$G$为单群，$G$的5阶西洛子群至少有6个，它们有$6\cdot 4+1=25$个元素。上述所有子群的任意两个均只有公共元素$1_G$，从而总共有$46+25-1=68$个元素。但是$|G|=60$，这一矛盾表明必有两个不同的4阶西洛子群$P$和$P'$，使得$P\cap P'=K\neq\{1\}$。由于$P$和$P'$都是阿贝尔群，从而$\langle P, P'\rangle$是$C_G(K)$的子群。由于$P\neq P'$，从而$P$和$P'$生成的群$\langle P, P'\rangle$的阶大于4，于是$4<|C_G(K)|<15$，并且$4\,||C_G(K)||\,60$，于是$|C_G(K)|=12$。从而上面证明了$G$必有12阶子群（或者是$N_G(P)$或者是$C_G(K)$）。

现在设N为G的12阶子群。将G作用于G对于N的5个陪集上（作用是左乘），可得到同态$\rho: G\to S_5$。由于ρ是单同态，从而G同构于S_5的一个60阶（即指数为2）的子群M。但是M是S_5的非平凡正规子群，从而M必然为A_5（系2.1.1），从而G必然同构于A_5。这就完成了定理2.3.5的证明。

第三章　群的结构

本章进一步研究某些群的结构。首先在§3.1中介绍约束条件最少的群——自由群以及用定义关系刻划群结构的方法，在§3.2中讲述有限生成阿贝尔群的结构，然后在§3.3中决定阶数$\leqslant 15$的全部群，最后讲述幂零群和可解群的基本知识（§3.4）。

§3.1　自由群和群的表现

先研究什么是自由半群。设S为集合，S中有限个元素x_1，x_2，…，x_n连在一起$x_1x_2\cdots x_n$叫作是一个**字**。字$x_1\cdots x_n$和$y_1\cdots y_m$相等，指得是$n=m$，并且$x_i=y_i$（$1\leqslant i\leqslant n$）。以$\Sigma^*(S)$表示所有这样的字（包括**空字**1）组成的集合。在$\Sigma^*(S)$中定义两个字的运算为：

$$(x_1\cdots x_n)(y_1\cdots y_m)=x_1\cdots x_ny_1\cdots y_m,$$

并且对每个字$a\in\Sigma^*(S)$，规定$1\cdot a=a\cdot 1=a$，则这个运算显然满足结合律。从而$\Sigma^*(S)$对于上述运算形成一个含幺半群，称作是集合S上的**自由含幺半群**，而集合S叫做$\Sigma^*(S)$的**基**。“自由”一字意味着：$\Sigma^*(S)$中除了含幺半群定义中的要求之外，没有任何其他约束条件。

如果将自由含幺半群$\Sigma^*(S)$扩大成群，每个元素$x\in S$应当有逆元素，所以给了集合S之后，再考虑集合$S^{-1}=\{x^{-1}|x\in S\}$。令

$$F(S)=\{a_1\cdots a_n|a_i\in S\cup S^{-1}(1\leqslant i\leqslant n)\}$$

这里当$n=0$时，规定$a_1\cdots a_n=1$。$F(S)$中运算仍定义为$(a_1\cdots a_n)(b_1\cdots b_m)=a_1\cdots a_nb_1\cdots b_m$，但是约定$aa^{-1}=a^{-1}a=1$，$1a=a1=a$（对每个$a\in F(S)$）。例如，$(ab)(b^{-1}c)=abb^{-1}c=a1c=ac$，$(ab)(b^{-1}a^{-1})=abb^{-1}a^{-1}=a1a^{-1}=aa^{-1}=1$等等。这时，$F(S)$中

每个元素均有逆元素。例如a^{-1}的逆元素为a，而$(a^3b^{-1}c)^{-1}=c^{-1}ba^{-3}$（其中$a^3=aaa$，$a^{-3}=a^{-1}a^{-1}a^{-1}$等等），于是$F(S)$对于上述运算和约定形成群，叫做**集合$S$上的自由群**，$S$叫作此自由群的基。显然$S$是群$F(S)$的一个生成元系。如果$S$是有限集，则$F(S)$叫作**有限生成自由群**。特别当$S=\{a\}$时，$F(S)=\langle a\rangle=\{a^n|n\in\mathbb{Z}\}$就是无限循环群。而当$|S|\geqslant 2$时，$F(S)$是无限非阿贝尔群。

下面定理看出自由群的作用。

定理3.1.1 每个群都是自由群的商群，每个有限生成群都是有限生成自由群的商群。

证明 设G为群，取G的一个生成元系Σ（例如可取$\Sigma=G$）。定义集合 $S=\{X_a|a\in\Sigma\}$并考虑映射f：$F(S)\to G$，其中$f(X_a)=a$，$f(X_a^{-1})=a^{-1}$，然后对于$A_i\in\Sigma\cup\Sigma^{-1}$，$(1\leqslant i\leqslant n)$，定义$f(A_1\cdots A_n)=f(A_1)\cdots f(A_n)$。这个映射是可以定义的，即不依赖于$F(S)$中元素的不同表达方式。因为这种不同表达方式是由于插入或消去$X_aX_a^{-1}$或$X_a^{-1}X_a$造成的，而$f(X_aX_a^{-1})=aa^{-1}=1$，$f(X_a^{-1}X_a)=f(X_a^{-1})f(X_a)=a^{-1}a=1$。进而，易知$f$为群的同态，并且是满同态，因为对每个生成元$a\in S$，$a=f(X_a)\in\mathrm{Im}f$，从而$G=\langle S\rangle=\mathrm{Im}f$。于是由同态基本定理，$G\cong F(S)/\mathrm{Ker}f$，即$G$同构于自由群$F(S)$的商群。如果$G$是有限生成群，令有限集$\Sigma$是$G$的一个生成元系，则$S=\{X_a|a\in S\}$也是有限集，从而$F(S)$是有限生成自由群。证毕。

设G同构于自由群$F(S)$的商群，f：$F(S)/K\cong G$，$K\lhd F(S)$，则G是由$f(S)=\Sigma$生成的。进而，对于K中每个元素a，在G中就有一个等式$f(a)=1_G$。例如若a，$b\in S$，$ab\in K$。令$f(a)=A$，$f(b)=B$，则在G中$AB=1$。K中有多少元素，G中就相应有多少个关系。如果P是K的一个子集，并且K是$F(S)$中包含P的最小正规子群（叫作**由P生成的正规子群**），则K中每个元素均可由P在$F(S)$中的全部共轭集合的元素运算出来。反映在群G中，G的所有关系均可由P中元素

给出的关系推导出来。把由P中元素给出的那些关系全体叫作群G的**定义关系集**，并且群G写成：

$$G=\langle\Sigma\,|\,f(\alpha)=1\ \ (\text{对每个}\ \alpha\in P)\rangle$$

这种刻划群G的方式叫作群G的一个表现。例如令$S=\{a,b\}$，K是$F(S)$中由元素a^3和$(ab)^2$生成的正规子群。如果$G\cong F(S)/K$，则G的结构可以写成$G=\langle A,\ B\,|\,A^3=(AB)^2=1\rangle$。

例3.1.1 $G=\langle S\,|\,\varnothing\rangle$（$\varnothing$表示的关系集合为空集)，即是以$S$为基的自由群。因为此时$K=\{1\}$，而$G\cong F(S)\{1\}=F(S)$。

例3.1.2 $Z_n\cong\langle a\rangle/\langle a^n\rangle=F(S)/\langle a^n\rangle$，其中$S=\{a\}$，从而$n$阶循环群的表现为$Z_n=\langle a\,|\,a^n=1\rangle$。

例3.1.3 $n\geqslant 3$正n边形对称群D_n是$2n$阶群。如例2.2.4所示，它有生成元系$\{\sigma,\ \tau\}$，其中$\sigma^n=1$，$\tau^2=1$，$(\tau\sigma)^2=1$。令F是以$\{a,\ b\}$为基的自由群，则有群的满同态：

$$f:\ F\to D_n,\quad f(a)=\sigma,\quad f(b)=\tau。$$

由同态基本定理可知，有同构$F/\mathrm{Ker}\,f\simeq D_n$。由于$f(a^n)=\sigma^n=1$，$f(b^2)=\tau^2=1$，$f((ba)^2)=(\tau\sigma)^2=1$，从而$a^n$，$b^2$，$(ba)^2\in\mathrm{Ker}\,f$。令$K$是$F$中由$a^n$，$b^2$和$(ba)^2$生成的正规子群，则$K\leqslant\mathrm{Ker}\,f$。

现在考虑商群F/K。以A和B分别表示a和b在F/K中的像，则$A^n=B^2=(BA)^2=1$，而F/K可由$\{A,\ B\}$生成。由于$BA=A^{-1}B^{-1}=A^{n-1}B$，可知F/K中元素均可表成A^iB^j($0\leqslant i\leqslant n-1$，$0\leqslant j\leqslant 1$)，从而$|F/K|\leqslant 2n$。于是

$$2n=|D_n|=|F/\mathrm{Ker}\,f|=\frac{|F/K|}{|\mathrm{Ker}\,f/K|}\leqslant 2n/|\mathrm{Ker}\,f/K|$$

从而$|\mathrm{Ker}f/K|=1$，即$K=\mathrm{Ker}\,f$。因此$D_n\cong F/K$，即D_n有如下的表现

$$D_n=\langle a,\ b\,|\,a^n=b^2=(ba)^2=1\rangle。$$

例3.1.4 令$Q_8=\langle a,\ b\,|\,a^4=1,\ b^2=a^2,\ ba=a^3b\rangle$，$Q_8$中每元均可写成$a^ib^j$（$0\leqslant i\leqslant 3$，$0\leqslant j\leqslant 1$），从而$|Q_8|\leqslant 8$。现

有一个具体矩阵群$G=\langle A, B\rangle$，其中$A=\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$，$B=\begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$（$i=\sqrt{-1}$），满足$A^4=1$，$B^2=A^2$，$BA=A^3B$。并且可直接验证$A^iB^j$（$0\leqslant i\leqslant 3$，$0\leqslant j\leqslant 1$）为8个不同的矩阵，因此$|G|=8$。然后可按例3.1.3中同样方法得出$G\cong Q_8$，即$Q_8$为8阶（非阿贝尔）群。

定义3.1.1 设S为集合，表现为

$$F=\langle S|ba=ab \quad (\text{对任何 } a, \ b\in S)\rangle$$

的群叫作**以S为基（或在S上）的自由阿贝尔群**（除了交换性条件之外不再有任何关系）。由于元素可交换，所以F中元素均可写成

$$g=a_1^{n_1}a_2^{n_2}\cdots a_r^{n_r} \quad (r\geqslant 0\ n_i\in\mathbb{Z},\ n_i\neq 0\ \ (1\leqslant i\leqslant n))$$

其中a_1，…，a_r是S中不同元素，并且若不考虑前后次序，g的这个表达方式是唯一的。

可以像定理3.1.1那样证明：每个（有限生成）阿贝尔群均是(有限生成）自由阿贝尔群的商群。为了进一步看清有限生成自由阿贝尔群的结构和第四章的需要，现在引进群的直积和半直积的概念。

定义3.1.2 设G_1，…，G_n是群，在集合的积

$$G=G_1\times\cdots\times G_n=\{(g_1, \ \cdots, \ g_n)|g_i\in G_i(1\leqslant i\leqslant n)\}$$

中定义运算：

$$(g_1, \ \cdots, \ g_n)(g_1', \ \cdots, \ g_n')=(g_1g_1', \ \cdots, \ g_ng_n'),$$

易证G对此运算形成群，叫作群G_1，…，G_n的**直积**。其中幺元素为$(1_{G_1}, \ \cdots, \ 1_{G_n})$，元素$(g_1,\cdots,g_n)$的逆为$(g_1^{-1},\cdots, \ g_n^{-1})$。

设G和K是群，则$G\times 1=\{(g, \ 1)|g\in G\}$和$1\times K=\{(1, \ k)|k\in K\}$是$G\times K$的两个子群，并且$G\times 1\cong G$，$1\times K\cong K$。$G\times 1$中元素和$1\times K$中元素是可以交换的，$G\times K=(G\times 1)(1\times K)$，$(G\times 1)\cap(1\times K)=\{1\}$。反之有如下引理。

引理 3.1.1 设 H，$K\leqslant G$，$H\cap K=\{1\}$，$G=HK$，并且对每个 $h\in H$，$k\in K$，$hk=kh$，则 $G\cong H\times K$。

证明 由 $G=HK$ 和 H 中元素与 K 中元素的交换性，可知 G 中每个元素均可表成 $g=hk$，$h\in H$，$k\in K$。再由 $H\cap K=\{1\}$ 可知 g 的这个表达式是唯一的。因为若又有 $g=h'k'$，$h'\in H$，$k'\in K$，则 $hk=h'k'$，于是 $(h')^{-1}h=k'k^{-1}\in H\cap K=\{1\}$，从而 $h=h'$，$k=k'$。于是我们可以定义

$$f: G\to H\times K,\ hk\to (h,\ k)$$

由上述可知这是一一对应，并且

$$\begin{aligned} f((hk)(h'k')) &= f(hh'kk')=(hh',\ kk') \\ &=(h,\ k)(h',\ k') \\ &= f(hk)f(h'k') \end{aligned}$$

从而 f 为同构，即 $G\cong H\times K$。证毕。

练习3.1.1 设 G_1，G_2，G_3 为群，则

(a) $G_1\times G_2\cong G_2\times G_1$；

(b) $(G_1\times G_2)\times G_3\cong G_1\times(G_2\times G_3)\cong G_1\times G_2\times G_3$。

练习3.1.2 设 G_i $(1\leqslant i\leqslant n)$ 为群，则

(a) $C(G_1\times\cdots\times G_n)=C(G_1)\times\cdots\times C(G_n)$

(b) $G_1\times\cdots\times G_n$ 是阿贝尔群 $\Longleftrightarrow G_i$ $(1\leqslant i\leqslant n)$ 均为阿贝尔群。

练习3.1.3 设 $N_i\leqslant G_i$ $(1\leqslant i\leqslant n)$，则

(a) $N_1\times\cdots\times N_n\leqslant G_1\times\cdots\times G_n$；

(b) $N_1\times\cdots\times N_n\lhd G_1\times\cdots\times G_n\Longleftrightarrow N_i\lhd G_i$ $(1\leqslant i\leqslant n)$；

(c) 当 $N_1\times\cdots\times N_n\lhd G_1\times\cdots\times G_n$ 时，则

$(G_1\times\cdots\times G_n)/(N_1\times\cdots\times N_n)\cong(G_1/N_1)\times\cdots\times(G_n/N_n)$。

练习3.1.4 以 $\mathbb{C}^*$ 表示非零复数乘法群，$\mathbb{R}_{正}$ 为正实数乘法群，$\mathbb{R}$ 为实数加法群，则 $\mathbb{C}^*\cong\mathbb{R}_{正}\times(\mathbb{R}/2\pi\mathbb{R})$。

练习3.1.5 设 n_1，$\cdots$，n_r 为自然数，则

(a) $Z_{n_1}\times Z_{n_2}\cong Z_{n_1n_2}\Longleftrightarrow(n_1,\ n_2)=1$；

(b) 如果 n_1，$\cdots$，n_r 两两互素，则 $Z_{n_1}\times\cdots\times Z_{n_r}\cong Z_{n_1\cdots n_r}$。

定义3.1.3[●] 设H和K是群，而且对每个元素$h\in H$，有K的一个自同构$\hat{h}$：$K\to K$，记$\hat{h}(k)=k^h$，使得对任何h_1，$h_2\in H$，有

$$(k^{h_1})^{h_2}=k^{h_1h_2}。$$

在集合的积$H\times K$上定义运算：

$$(h_1,\ k_1)(h_2,\ k_2)=(h_1\cdot h_2,\ k_1^{h_2}\cdot k_2),$$

不难验证$H\times K$对此运算形成群，叫作H和K的**半直积**，用$H\rtimes K$表示。其中幺元素为(1，1)，元素$(h,\ k)$的逆为$(h^{-1},\ (k^{-1})h^{-1})$。

引理3.1.2 设H和K是群，G是H和K的半直积，即$G=H\rtimes K$，则$H_1=\{(h,\ 1)\in G\mid h\in H\}$和$K_1=\{(1,\ k)\in G\mid k\in K\}$是$G$的子群，而且$H_1\cong H$，$K_1\cong K$，$K_1$是$G$的正规子群和$H_1\cap K_1=\{(1,\ 1)\}$，$G=H_1\cdot K_1$。

证明 易见$H_1\cong H$，$K_1\cong K$和$H_1\cap K_1=\{(1,\ 1)\}$。由于$(h,\ 1)(1,\ k)=(h,\ k)$，于是$G=H_1\cdot K_1$。由于

$$(h,\ 1)^{-1}(1,\ k)(h,\ 1)=(1,\ k^h),$$

因此K_1是G的正规子群。

定理3.1.2 设H和K是群G的两个子群，当且仅当满足下面的条件时$G=H\rtimes K$。

(1) K是G的正规子群；

(2) $K\cap H=1$；

(3) $G=H\cdot K$。

证明： 只需证明充分性。

由于$K\cap H=1$，$G=H\cdot K$和K是正规的，则G的每个元素可以唯一地表成：

$$g=hk,$$

其中$h\in H$，$k\in K$。映射：$k\to h^{-1}kh$给出子群K的一个自同构，记$h^{-1}kh=k^h$。容易验证

● 在有些书中定义时，H与K的顺序与本书相反。

$$(k^{h_1})^{h_2}=k^{h_1h_2}$$

对于G的两个元素的积表示：

$$g_1=h_1k_1,\quad g_2=h_2k_2,$$

计算

$$g_1\cdot g_2=h_1k_1h_2k_2=h_1h_2(h_2^{-1}k_1h_2)k_2=h_1h_2\cdot k_1^{h_2}k_2,$$

因此$G=H\rtimes K$。

下面定理是判别一个群为某些子群直积的方法。以后将$G=G_1\times\cdots\times G_n$中元素（$g_1$，1，…，1）等同于$G_1$中元素$g_1$，由此将$G_1$看成是$G$的(正规)子群。类似地，$G_2$，…，$G_n$也自然地看成是$G$的（正规）子群，从而$G$中每个元素唯一地表示成$g=g_1\cdots g_n$（$g_i\in G_i$）。

定理3.1.3 设G_1，…，$G_n\lhd G$，$n\geqslant 2$，则以下三条件是彼此等价的。

（1）$G=G_1\times\cdots\times G_n$；

（2）G中每个元素可以唯一表示成$g=g_1\cdots g_n(g_i\in G_i)$；

（3）$G=G_1\cdots G_n$，并且对每个m（$1<m\leqslant n$），$(G_1G_2\cdots G_{m-1})\cap G_m=\{1\}$。

证明 （1）⇒（2）：如本定理前面的约定，G中元素（g_1，…，g_n）唯一地写成

$$\begin{aligned}(g_1,\cdots,g_n)&=(g_1,1,\cdots,1)\cdots(1,1,\cdots,1,g_n)\\&=g_1\cdots g_n\text{。}\end{aligned}$$

（2）⇒（3）：设$g\in(G_1\cdots G_{m-1})\cap G_m$，则有$g_i\in G_i$（$1\leqslant i\leqslant m$），使得$g_m=g=g_1\cdots g_{m-1}$，于是$1=g_1\cdots g_{m-1}g_m^{-1}\cdot 1_{G_{m+1}}\cdots 1_{G_n}$。由（2）中唯一性假设可知$g_m^{-1}=1$，从而$g=g_m=1$，于是$(G_1\cdots G_{m-1})\cap G_m=\{1\}(2\leqslant m\leqslant n)$。

（3）⇒（1）：令$J_m=G_1\cdots G_m$ 由$G_i\lhd G$（$1\leqslant i\leqslant n$）可知$J_m\lhd G$，现在对m归纳证明$J_m=G_1\times\cdots\times G_m$（$2\leqslant m\leqslant n$）。当$m=2$时，由引理3.1.1可知$J_2=G_1\times G_2$。现在设$J_{m-1}=G_1\times\cdots\times G_{m-1}$，则$J_{m-1}$，$G_m\lhd J_m$，$J_m=J_{m-1}G_m$，并且由（3）中假设，$J_{m-1}\cap G=\{1\}$，于是又由引理3.1.1可知，$J_m=J_{m-1}\times G_m=G_1$

$\times\cdots\times G_m$，特别地对于 $m=n$，即得 $G=J_n=G_1\times\cdots\times G_n$。证毕。

现在回到有限生成自由阿贝尔群 G。设它的基为 $S=\{a_1,\cdots a_r\}$，则 G 中每个元素唯一表示成 $g=a_1^{\lambda_1}\cdots a_r^{\lambda_r}(\lambda_i\in\mathbb{Z}(1\leqslant i\leqslant r))$。由于阿贝尔群 G 的子群 $G_i=\langle a_i\rangle$ 均是正规的，从而由定理3.1.2的（2）即知 $G=G_1\times\cdots\times G_r$。但是 $G_i=\langle a_i\rangle$ 是无限循环群，从而 G 同构于 r 个有限循环群的直积。

对于每个群 G，今后把 n 个群 G 的直积写成 G^n，而 $G_n=\{g^n|g\in G\}$。当 G 为阿贝尔群时，G_n 是 G 的子群。现在设 G 是有限生成自由阿贝尔群，则 $G=\langle a_1\rangle\times\cdots\times\langle a_r\rangle\cong Z^r$，其中 $\langle a_i\rangle$ 均是无限循环群，于是对每个 $n\geqslant 2$，$G_n=\langle a_1^n\rangle\times\cdots\times\langle a_r^n\rangle$，和 $G/G_n\cong(\langle a_1\rangle/\langle a_1^n\rangle)\times\cdots\times(\langle a_r\rangle/\langle a_r^n\rangle)\cong Z_n\times\cdots\times Z_n\cong Z_n^r$，$|G/G_n|=|Z_n^r|=|Z_n|^r=n^r$，于是数 $r=\log|G/G_n|/\log n$ 是由群 G 本身所唯一决定的。换句话说，如果 $G\cong Z^r$，并且 $G\cong Z^s$，则必然 $r=s$。所以，有限生成自由阿贝尔群本质上是 Z^r（$r=1,2,3,\cdots$），并且它们彼此互不同构。

如果 $G\cong Z^r$，则 r 叫作有限生成自由阿贝尔群 G 的秩，表示成 $\mathrm{rank}\,G$。综合上述，证明了下面的结构定理。

定理3.1.4 有限生成自由阿贝尔群 G 同构于有限个无限循环群的直积：$G\cong Z^r$，$r=\mathrm{rank}\,G\geqslant 1$。并且两个这样的群 G 和 G' 同构 $\Longleftrightarrow \mathrm{rank}\,G=\mathrm{rank}\,G'$。

系3.1.1 设 S 和 S' 是有限生成自由阿贝尔群 G 的两组基，则 $|S|=|S'|$。

上面给出了有限生成自由阿贝尔群的结构（或叫分类），下一节将要给出任意有限生成阿贝尔群的结构（分类）。

§3.2 有限生成阿贝尔群结构

在本节中，像通常所作的那样，把阿贝尔群 A 中运算写成加法形式，从而幺元素为 0，元素 a 的逆是 $-a$，n 个 a 运算为 $a+a+\cdots+a=na$（不是 a^n），从而有限阶元素 a 的阶为满足

$na=0$ 的最小正整数（对于无限阶元素 a，满足 $na=0$ 的正整数 n 不存在）。$nA=\{na|a\in A\}$，直积则改叫作**直和**，并且写成 $A\oplus A'$。n 个 A 的直和仍表成 A^n。

下一个定理是研究有限生成阿贝尔群结构最基本的定理。

定理3.2.1 有限生成自由阿贝尔群 F 的每个子群 $G(G\neq\{0\})$ 仍是有限生成自由阿贝尔群，并且 $\mathrm{rank}G\leqslant\mathrm{rank}F$。更确切地说，令 $n=\mathrm{rank}F$，则存在 F 的一组基 $\{x_1, \cdots, x_n\}$，一个整数 $r(1\leqslant r\leqslant n)$ 和一组正整数 $d_1, \cdots, d_r$，使得 $d_1|d_2|\cdots|d_r$，并且 G 是以 $\{d_1x_1, \cdots, d_rx_r\}$ 为基的自由阿贝尔群。

证明 当 $n=1$ 时，由无限循环群的子群特性可知定理3.2.1成立，现在假设定理 3.2.1 对于秩小于 n 的所有自由阿贝尔群均成立。以 S 表示集合

$$\left\{s\in\mathbb{Z}\,\middle|\,\begin{array}{l}\text{存在}F\text{的一组基}\{y_1, \cdots, y_n\}\text{，使得}G\text{中有形如}\\ sy_1+k_2y_2+\cdots+k_ny_n(k_i\in\mathbb{Z})\text{ 的元素}\end{array}\right\}$$

注意 $\{y_2, y_1, y_3, \cdots, y_n\}$ 也是 F 的一组基，从而 $k_2\in S$。类似地 $k_i\in S(3\leqslant i\leqslant n)$。由于 $G\neq\{0\}$，从而 S 中有非零整数。并且易知若 $s_1, s_2\in S$，则 $-s_1, s_1\pm s_2\in S$，从而 S 中有正整数。以 d_1 表示 S 中最小正整数，于是存在 $v=d_1y_1+k_2y_2+\cdots+k_ny_n\in G$。令 $k_i=d_1q_i+r_i(0\leqslant r_i<d_1)$，则 $v=d_1(y_1+q_2y_2+\cdots+q_ny_n)+r_2y_2+\cdots+r_ny_n$。易知 $(x_1=y_1+q_2y_2+\cdots+q_ny_n, y_2, \cdots, y_n)$ 也是 F 的一组基，从而 $r_i\in S(2\leqslant i\leqslant n)$。由 d_1 的极小性可知 $r_i=0(2\leqslant i\leqslant n)$，于是 $v=d_1x_1\in G$。

令 $H=\langle y_2, \cdots, y_n\rangle$，这是秩 $n-1$ 的自由阿贝尔群，现在证明 $G=\langle V\rangle\oplus(G\cap H)=\langle d_1x_1\rangle\oplus(G\cap H)$。首先，由于 $\{x_1, y_2, \cdots, y_n\}$ 为 F 的一组基，从而 $\langle V\rangle\cap(G\cap H)=\{0\}$。其次，对每个元素 $u=t_1x_1+t_2y_2+\cdots+t_ny_n\in G(t_i\in\mathbb{Z})$，令 $t_1=d_1q_1+r_1, 0\leqslant r_1<d_1$，则 $u-q_1v=r_1x_1+t_2y_2+\cdots+t_ny_n\in G$。由 d_1 的极小性知 $r_1=0$，于是 $t_2y_2+\cdots+t_ny_n\in G\cap H$，而 $u=q_1v+(t_2y_2+\cdots+t_ny_n)\in\langle v\rangle+(G\cap H)$。综上可知 $G=\langle d_1x_1\rangle\oplus(G\cap H)$。

如果$G\cap H=\{0\}$，则$G=\langle d_1x_1\rangle$，从而定理成立。如果$G\cap H\neq\{0\}$，则$G\cap H$是秩为$n-1$的自由阿贝尔群H的子群，根据归纳假设可知存在H的一组基$\{x_2, \cdots, x_n\}$，正数r $(r-1\leqslant n-1)$，$d_2, \cdots, d_r$，使得$d_2|d_3|\cdots|d_r$，并且$G\cap H=\langle d_2x_2\rangle\oplus\cdots\oplus\langle d_rx_r\rangle$，于是$F=\langle x_1\rangle\oplus\cdots\oplus\langle x_n\rangle$，$G=\langle d_1x_1\rangle\oplus\cdots\oplus\langle d_rx_r\rangle$。只需再证$d_1|d_2$。令$d_2=qd_1+r_0$，$0\leqslant r_0<d_1$，则$\{x_2, x_1+qx_2, x_3, \cdots, x_n\}$为$F$的一组基，$r_0x_2+d_1(x_1+qx_2)=d_1x_1+d_2x_2\in G$，从而$r_0\in S$。由$d_1$的最小性知$r_0=0$，即$d_1|d_2$。证毕。

练习3.2.1 阿贝尔群F的子集X叫作**线性无关**的是指，若$n_1x_1+\cdots+n_rx_r=0$，其中$n_i\in\mathbb{Z}$，$x_1, \cdots, x_r$是X中不同的元素，则$n_1=\cdots=n_r=0$。求证：

（a）X是线性无关的$\Longleftrightarrow$子群$\langle X\rangle$中每个非零元素均可唯一写成$n_1x_1+\cdots+n_rx_r$，其中$n_i\in\mathbb{Z}$，$n_i\neq 0$，而$x_1, \cdots, x_r$为X中不同元素。

（b）设F是有限生成自由阿贝尔群，$\operatorname{rank}F=n$，则F中n元线性无关子集不一定是F的一组基，F的生成元系也不一定包含F的一组基。但是$\operatorname{rank}F$等于F中线性无关子集元素个数的最大值。

练习3.2.2 （a）证明有理数加法群$\mathbb{Q}$不是自由阿贝尔群，也不是有限生成的。

（b）证明非零有理数乘法群$\mathbb{Q}^*$是以全部素数为基的自由阿贝尔群。

练习3.2.3 有限生成阿贝尔群A是自由的$\Longleftrightarrow A$中每个非零元素都是无限阶的。

定理3.2.2 每个有限生成阿贝尔群A均同构于$\mathbb{Z}^r\oplus Z_{m_1}\oplus\cdots\oplus Z_{m_t}$，其中$r$，$t\geqslant 0$，$1<m_1\leqslant\cdots\leqslant m_t$，并且$m_1|m_2|\cdots|m_t$。

证明 不妨设$A\neq\{0\}$，并且设A是由n个元素生成的，则A同构于秩为n的自由阿贝尔群F的商群$A\cong F/K$。如果$K=\{0\}$，则$A\cong F$，此为定理中$r=n$，$t=0$的情形。如果F的

子群$K\neq\{0\}$，则由定理 3.2.1 可知存在$x_1, \cdots, x_n\in F$，正整数$d_1, \cdots, d_s(1\leqslant s\leqslant n)$，$d_1|d_2|\cdots|d_s$，使得$F=\langle x_1\rangle\oplus\cdots\oplus\langle x_n\rangle$，$K=\langle d_1x_1\rangle\oplus\cdots\oplus\langle d_nx_n\rangle$，其中令$d_{s+1}=\cdots=d_n=0$。从而

$$G\cong F/K\cong(\langle x_1\rangle/\langle d_1x_1\rangle)\oplus\cdots\oplus(\langle x_n\rangle/\langle d_nx_n\rangle)$$
$$\cong(\langle x_1\rangle/\langle d_1x_1\rangle)\oplus\cdots\oplus(\langle x_s\rangle/\langle d_sx_s\rangle)\oplus\mathbb{Z}^{n-s}。$$

注意$\langle x_1\rangle/\langle x_1\rangle=\{0\}$，从而以$m_1, \cdots, m_t$表示$d_1, \cdots, d_s$中不为 1 的那些正整数，则$G\cong\mathbb{Z}^r\oplus Z_{m_1}\oplus\cdots\oplus Z_{m_t}$（其中$r=n-s$），并且$m_1|m_2|\cdots|m_t$。证毕。

设A是有限生成阿贝尔群。以A_t表示A中有限阶元素全体。如果a和b是A中阶数分别为r和s的元素，则a^{-1}和ab的阶分别是r和$[r, s]$（r和s的最小公倍数）的因子，从而A_t是A的子群，叫作A的**扭子群**。

定理3.2.3 设A和B是有限生成阿贝尔群。

（1）存在A的有限生成自由阿贝尔子群A_f，使得$A=A_f\oplus A_t$。

（2）如果$A=A_f\oplus A_t$，$B=B_f\oplus B_t$，其中A_f和B_f分别为A_f和B_f的有限生成自由阿贝尔子群，则$A\cong B\Longleftrightarrow\text{rank}A_f=\text{rank}B_f$，并且$A_t\cong B_t$。

证明（1）根据定理 3.2.2 可知$A\overset{f}{\xrightarrow{\sim}}\mathbb{Z}^r\oplus T$，其中$T=Z_{m_1}\oplus\cdots\oplus Z_{m_t}$，$1<m_1|m_2|\cdots|m_t$。不难看出，$\mathbb{Z}^r\oplus T$的扭子群就是$T$。同构$f$把$A$中$r$阶元素映为$r$阶元素，从而$f^{-1}(T)$就是$A$的扭子群$A_t$。令$f(\mathbb{Z}^r)=A_f$，则$A_f\cong\mathbb{Z}^r$，且$A=A_f\oplus A_t$。

（2）如果$A\overset{f}{\xrightarrow{\sim}}B$，则$A_f\oplus A_t\cong B_f\oplus B_t$。由于$A_t\overset{f}{\xrightarrow{\sim}}B_t$，从而$A_f\cong(A_f\oplus A_t)/A_t\cong(B_f\oplus B_t)/B_t\cong B_f$，于是$\text{rank}A_f=\text{rank}B_f$。反之，若$\text{rank}A_f=\text{rank}B_f$，则$A_f\cong B_f$。如果又有$A_t\cong B_t$，则$A=A_f\oplus A_t\cong B_f\oplus B_t=B$。证毕。

根据定理 3.2.3，每个有限生成阿贝尔群A均同构于$\mathbb{Z}^r\oplus A_t$，其中r是由A唯一决定的，叫作A的**秩**，表示成$\text{rank}A$。当A为有限生成自由阿贝尔群时，$A_t=\{1\}$，可知这里秩的定义与

对自由阿贝尔群情形的定义是一致的。从而定理3.2.3的（2）可简述为：设A和B是两个有限生成阿贝尔群，则$A\cong B\Longleftrightarrow \text{rank}A=\text{rank}B$，并且$A_t\cong B_t$，于是问题便化为有限阿贝尔群$A_t$的分类问题。

定理3.2.4 设A为有限阿贝尔群，$A\neq\{0\}$，则：

（1）存在$1<m_1|m_2|\cdots|m_t$（$t\geqslant 1$），使得$A\cong Z_{m_1}\oplus\cdots\oplus Z_{m_t}$，且（$m_1$，…，$m_t$）是由$A$唯一决定。

（2）存在一组正整数$\{p_1^{s_1}, p_2^{s_2}, \cdots, p_k^{s_k}\}$，其中$p_1$，…，$p_k$为（不必不同的）素数，$s_1$，…，$s_k$为（不必不同的）正整数，使得$A\cong Z_{p_1^{s_1}}\oplus\cdots\oplus Z_{p_k^{s_k}}$，且集合$\{p_1^{s_1}, \cdots, p_k^{s_k}\}$是由群$A$唯一决定。

证明 有限阿贝尔群当然是有限生成的。由定理3.2.2，$A\cong \mathbb{Z}^r\oplus Z_{m_1}\oplus\cdots\oplus Z_{m_t}$。当$r>0$时，由于$\mathbb{Z}^r$中元素除0之外均为无限阶元素。而有限群$A$中元素均是有限阶的，于是$r=0$，即$A\cong Z_{m_1}\oplus\cdots\oplus Z_{m_t}$。从而得到（1）中的分解式。令$m_1=p_1^{\lambda_1}\cdots p_l^{\lambda_l}$，其中$p_1$，…，$p_l$是彼此不同的素数，而$\lambda_i$均为正整数，则$Z_{m_1}\cong Z_{p_1^{\lambda_1}}\oplus\cdots\oplus Z_{p_l^{\lambda_l}}$。将$Z_{m_2}$，…，$Z_{m_t}$也如此作成一些素数幂阶的循环群的直和，于是便得到（2）中的分解式。剩下只需再证满足定理条件的$\{m_1, \cdots, m_t\}$和$\{p_1^{s_1}, \cdots, p_k^{s_k}\}$的唯一性。

先证$\{p_1^{s_1}, \cdots, p_k^{s_k}\}$的唯一性。已知对于每个素数$p$，有限群$G$的西洛$p$-子群是彼此共轭的，且$G$中每个阶为$p$方幂的元素均在$G$的某个西洛$p$-子群之中。当$G$为有限阿贝尔群时，每个子群均只与自己共轭，从而对$|G|$的每个素因子$p$，$G$只有唯一的一个西洛$p$-子群$G_p$，并且$G_p$就是$G$中全部$p$方幂阶元素所构成的子群。设$|G|=p_1^{\lambda_1}, p_s^{\lambda_s}$是$|G|$的素因子分解式，则$|G_{p_i}|=p_i^{\lambda_i}$。由于$G_{p_i}$的阶两两互素，不难看出$G_{p_1}\cdots G_{p_{m-1}}\cap G_{p_m}=\{0\}$（$2\leqslant m\leqslant s$）。因此，$G_{p_1}\cdots G_{p_s}=G_{p_1}\oplus\cdots\oplus G_{p_s}$。但是，$|G_{p_1}\oplus\cdots\oplus G_{p_s}|=p_1^{\lambda_1}\cdots p_s^{\lambda_s}=|G|$，从而$G=G_{p_1}\oplus\cdots\oplus G_{p_s}$，即每个有限阿贝尔群是它的所有西洛子群的直和。对有限阿贝尔群A证明$\{p_1^{s_1}, \cdots, p_k^{s_k}\}$的唯一性，只需对它的每个西洛子群$A_p$证明

$\{p_1^{s_1}, \cdots, p_k^{s_k}\}$的唯一性即可。为此，设$A$为有限阿贝尔$p$-群（一个群叫作$p$-群，是指群中每个元素的阶均是素数$p$的方幂），这时，$A \cong Z_{p^{a_1}} \oplus \cdots \oplus Z_{p^{a_r}}$。现只需证明$\{a_1, \cdots, a_r\}$的唯一性。不妨设$1 \leqslant a_1 \leqslant a_2 \leqslant \cdots \leqslant a_r$，又有$A \cong Z_{p^{c_1}} \oplus \cdots \oplus Z_{p^{c_d}}$，$1 \leqslant c_1 \leqslant \cdots \leqslant c_d$，则$pA = pZ_{p^{a_1}} \oplus \cdots \oplus pZ_{p^{a_r}}$。于是$A/pA \cong \left(\frac{Z_{p^{a_1}}}{pZ_{p^{a_1}}}\right) \oplus \cdots \oplus \left(\frac{Z_{p^{a_r}}}{pZ_{p^{a_r}}}\right)$，但是$Z_{p^a}/pZ_{p^a} \cong \frac{\mathbb{Z}/p^a\mathbb{Z}}{p\mathbb{Z}/p^a\mathbb{Z}} \cong \mathbb{Z}/p\mathbb{Z} \cong Z_p$，于是$A/pA \cong Z_p^r$，从而$|A/pA| = p^r$。类似地由$A \cong Z_{p^{c_1}} \oplus \cdots \oplus Z_{p_1^{c_d}}$得到$|A/pA| = p^d$，由此首先得出$r = d$。

现在假设$a_1 = c_1, \cdots, a_{v-1} = c_{v-1}$，而$a_v < c_v$，则$p^{a_v}A \cong p^{a_v} \times Z_{p^{a_1}} \oplus \cdots \oplus p^{a_v}Z_{p^{a_r}} \cong Z_{p^{a_{v+1}-a_v}} \oplus \cdots \oplus Z_{p^{a_r-a_v}}$。同样有$p^{a_v}A \cong p^{a_v}Z_{p^{c_1}} \oplus \cdots \oplus p^{a_v}Z_{p^{c_r}} \cong Z_{p^{c_v-a_v}} \oplus Z_{p^{c_{v+1}-a_v}} \oplus \cdots \oplus Z_{p^{c_v-a_v}}$。由于$c_v - a_v, \cdots, c_r - a_v$均为正整数，从而$\frac{p^{a_v}A}{p^{a_v+1}A} \cong Z_p^{r-v+1}$。但是$a_{v+1} - a_v, \cdots, a_r - a_v$中共有$r - v$个数，于是$\frac{p^{a_v}A}{p^{a_v+1}A}$又同构于不超过$r - v$个$Z_p$的直和。这就导致矛盾。从而必然$a_i = c_i (1 \leqslant i \leqslant r)$，由此证明了$\{p_1^{s_1}, \cdots, p_k^{s_k}\}$的唯一性。

最后证明$\{m_1, \cdots, m_t\}$的唯一性。设$p_1, \cdots, p_r$是$|A| = m_1 m_2 \cdots m_t$的全部素因子，令

$1 < m_i = p_1^{a_{i1}} \cdots p_r^{a_{ir}}$，$a_{ij} \geqslant 0 (1 \leqslant i \leqslant t)$。由$m_1 | m_2 | \cdots | m_t$可知$0 \leqslant a_{1j} \leqslant a_{2j} \leqslant \cdots \leqslant a_{tj} (1 \leqslant j \leqslant r)$，于是$Z_{m_i}$的西洛$p_j$-子群为$Z_{p_j^{a_{ij}}}$不难看出，$A = Z_{m_1} \oplus \cdots \oplus Z_{m_t}$的西洛$p_j$-子群$A_p$为$Z_{p_j^{a_{1j}}} \oplus Z_{p_j^{a_{2j}}} \oplus \cdots \oplus Z_{p_j^{a_{tj}}} (0 \leqslant a_{1j} \leqslant a_{2j} \leqslant \cdots \leqslant a_{tj})$。由上一段结果可知$a_{1j}, \cdots, a_{tj}$中不为0的那些已由$A_p$所唯一决定，因此$(a_{1j}, \cdots, a_{tj})$由$A$所唯一决定。由条件$m_i > 1$可知$t$和所有的$a_{ij}$均由$A$所唯一决定，因此$\{m_1, \cdots, m_t\}$由$A$所唯一决定，这就完成了定理3.2.4的证明。

定理3.2.4中的$\{m_1, \cdots, m_t\}$叫作A的**不变因子**，$\{p_1^{s_1}, \cdots,$

$p_k^{s_k}\}$叫作A的**初等因子**。对于有限生成阿贝尔群A，A_t的不变因子和初等因子也分别叫作A的不变因子和初等因子，综合上述，完成了如下有限生成阿贝尔群的结构定理。

定理3.2.5 两个有限生成阿贝尔群同构$\Longleftrightarrow$它们有相同的秩和初等因子$\Longleftrightarrow$它们有相同的秩和不变因子。特别是，两个有限阿贝尔群同构$\Longleftrightarrow$它们有相同的初等因子$\Longleftrightarrow$它们有相同的不变因子。

例3.2.1 1500阶有限阿贝尔群的分类。 设A为阿贝尔群，$|A|=1500=4\times3\times125$，于是$A$的西洛子群的阶分别为$|A_2|=4$，$|A_3|=3$，$|A_5|=125$。从而$A$的初等因子共有以下六种可能：$\{2,2,3,5,5,5\}$，$\{2,2,3,5,25\}$，$\{2,2,3,125\}$，$\{4,3,5,5,5\}$，$\{4,3,5,25\}$，$\{4,3,125\}$。所以，1500阶阿贝尔群共有六个：$Z_2^2\oplus Z_3\oplus Z_5^3$，$Z_2^2\oplus Z_3\oplus Z_5\oplus Z_{25}$，$Z_2^2\oplus Z_3\oplus Z_{125}$，$Z_4\oplus Z_3\oplus Z_5^3$，$Z_4\oplus Z_3\oplus Z_5\oplus Z_{25}$，$Z_4\oplus Z_3\oplus Z_{125}$。

将初等因子$\{2,2,3,5,5,5\}$化为不变因子则为：$t=3$，$m_3=2\times3\times5$，$m_2=2\times5$，$m_1=5$，即初等因子为$\{5,10,30\}$。于是$Z_2^2\oplus Z_3\oplus Z_5^3\cong Z_5\oplus Z_{10}\oplus Z_{30}$。而另外五个群的不变因子依次分别为：$\{10,150\}$，$\{2,750\}$，$\{5,5,60\}$，$\{5,300\}$，$\{1500\}$。

练习3.2.4 设A为有限阿贝尔群，则对于$|A|$的每个正因子d，A均有d阶子群和d阶商群。

练习3.2.5 设A为有限生成阿贝尔群，则$\mathrm{rank}A$等于A中线性无关子集元数的最大值。

练习3.2.6 求证当$(m,n)=1$时，$Z_m\oplus Z_n$的不变因子为$\{mn\}$。而当$(m,n)>1$时，$Z_m\oplus Z_n$的不变因子为$\{(m,n),[m,n]\}$。

练习3.2.7 设H是有限阿贝尔群A的子群，则A有子群同构于A/H。

练习3.2.8 有限阿贝尔群A若不是循环群，则必存在素数

p使得A有子群同构于Z_p^2。

练习3.2.9 求$Z_2 \oplus Z_9 \oplus Z_{35}$的初等因子和不变因子。

练习3.2.10 试问$Z_{p^3} \oplus Z_{p^2}$有多少p^2阶子群。

练习3.2.11 求证非零复数乘法群$\mathbb{C}^*$的每个有限子群都是循环群。

§3.3 小阶群的结构

本节将给出阶数≤15的所有群的结构，并讨论每个群的子群格，正规子群，因子群，共轭类和群的中心。由于阿贝尔群已由前节完全决定，所以主要考虑有限非阿贝尔群。

定理3.3.1 设G是$2p$阶非阿贝尔群，其中p是奇素数，则$G=D_p$，其中D_p是正p边形对称群。

证明 如前令$N(p)$表示G的p阶西洛子群的个数，则$N(p)=l_{p+1}|2$，从而$N(p)=1$，即令a为G中p阶元素，则$\langle a\rangle$是G的p阶正规子群。又由西洛定理，G中存在2阶元素b，显然$b\notin\langle a\rangle$。于是$2p=|G|\geqslant|\langle a, b\rangle|>|\langle a\rangle|=p$，从而$\langle a, b\rangle=G$。由于$\langle a\rangle$是正规子群，因此$bab^{-1}=a^l$(对某个$0\leqslant l\leqslant p-1$)，于是$a=b^2ab^{-2}=ba^lb^{-1}=(bab^{-1})^l=a^{l^2}$，所以$l^2\equiv 1 \pmod p$，即$l\equiv\pm 1 \pmod p$。当$l\equiv 1 \pmod p$时，$ba=ab$。由于$a$和$b$生成$G$，这时$G$为阿贝尔群。若$bab^{-1}=a^{-1}$，则群$G$即为$\langle a, b \mid a^p=b^2=1, ba=a^{-1}b\rangle=D_p$。证毕。

定理3.3.2 设p和q为素数，$p>q$，$q\nmid p-1$，则pq阶群G必是循环群Z_{pq}。

证明 类似于定理3.3.1的证明，可知G中存在p阶元素a，并且$\langle a\rangle$是G的正规子群。另一方面，$N(q)=lq+1|p$，所以$N(q)=1$或p。若$lq+1=N(q)=p$，则$q|p-1$。与假设矛盾。从而$N(q)=1$，即G中存在q阶元素b，并且$\langle b\rangle$也是G的正规子群。显然$\langle a\rangle\cap\langle b\rangle=\{1\}$，$G=\langle a, b\rangle$，并且$bab^{-1}a^{-1}\in\langle a\rangle\cap\langle b\rangle$，从而$bab^{-1}a^{-1}=1$，即$ba=ab$。因此$G$为阿贝尔群，$Z_p\times Z_q=Z_{pq}$。证毕。

下面具体给出1到15阶群的结构。

3.3.1 若群G的阶$|G|=p$是素数，则G同构于p阶循环群Z_p。G是单群。G的子群格为

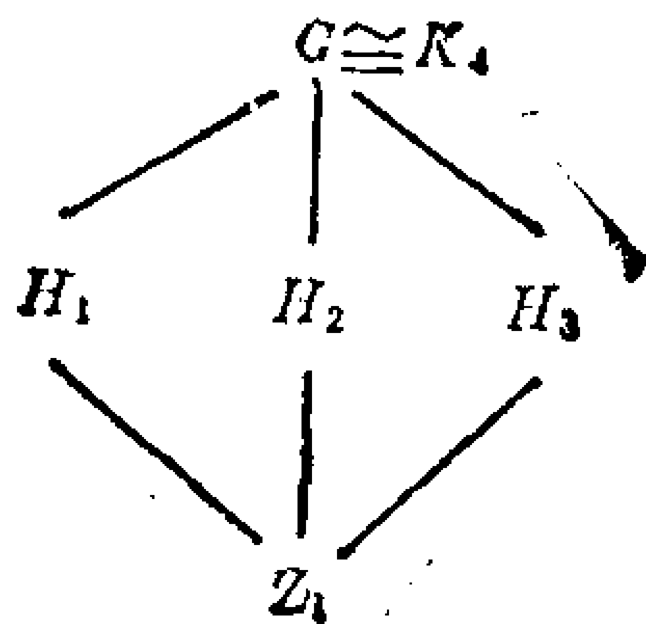
$$\begin{array}{c} G \\ | \\ Z_1 \end{array}$$

其中Z_1是只有1个单位元的平凡群。由此可知，阶为2，3，5，7，11，13的群的结构完全决定，它们都是单群，分别同构于Z_2，Z_3，Z_5，Z_7，Z_{11}，Z_{13}。

3.3.2 已知，若p是素数，则p^2阶群是阿贝尔群。由有限阿贝尔群的基本定理（见定理3.2.2)，可得$G\cong Z_{p^2}$或者$G\cong Z_p\times Z_p$。于是4阶群G或者同构于Z_4，这时其子群格是

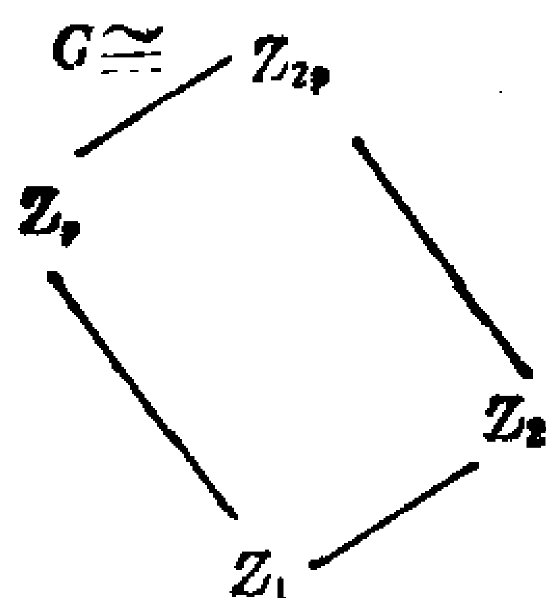
$$\begin{array}{c} G\cong Z_4 \\ | \\ Z_2 \\ | \\ Z_1 \end{array}$$

或者同构于克莱因4元群K_4。这时G有3个不同的2阶子群H_1、H_2、H_3，它们都同构于Z_2，因而其子群格是



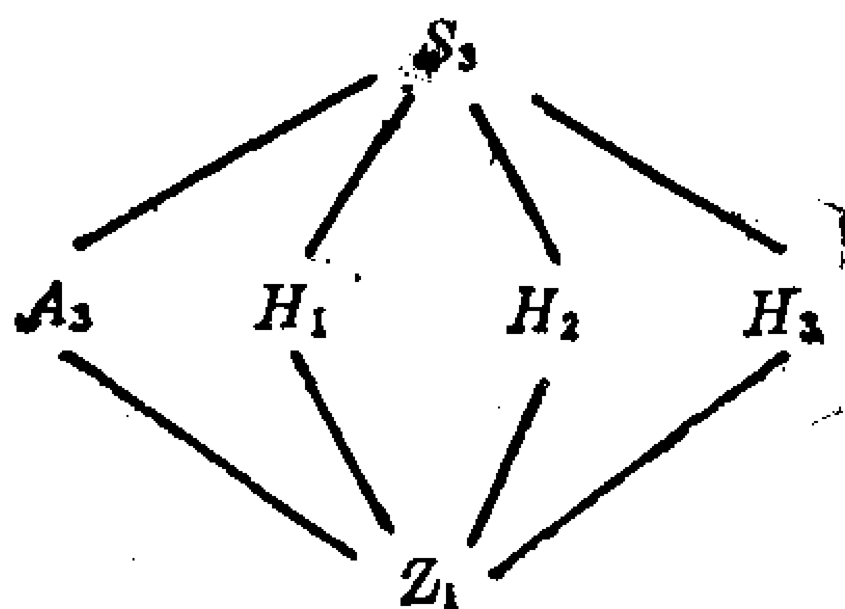
对于阶为$9=3^2$的群G，情形与阶为$4=2^2$的群完全相同。这时$G\cong Z_9$或者$G\cong Z_3\times Z_3$。

3.3.3 对于$2p$阶阿贝尔群G，其中p是奇素数则有$G\cong Z_{2q}\cong Z_2\times Z_q$，这时子群格为



因此阶为 6，10，14 的阿贝尔群分别同构于群 $Z_2\times Z_3$，$Z_2\times Z_5$，$Z_2\times Z_7$。对于 $2p$ 阶非阿贝尔群 G，其中 p 是奇素数，其结构由定理 3.3.1 确定。详细地说，有：

3.3.3.1　6 阶非阿贝尔群 G 同构于对称群 S_3，即 $G\cong S_3$。事实上，$G=\{a,\ b\mid a^2=b^3=1,\ aba^{-1}=b^2\}$，$S_3=\{(12),(123)\mid (12)^2=(123)^3=1,(12)(123)(12)^{-1}=(123)^2\}$。$S_3$ 是最小的非阿贝尔群。S_3 有 3 个共轭类，它们是 $\{(1)\}$，$\{(12),(13),(23)\}$，$\{(123),(321)\}$。S_3 的中心 $C(S_3)=\{(1)\}$。S_3 的换位子群 $S_3'=[S_3,\ S_3]=A_3=\{(1),(123),(321)\}$。$S_3$ 的正规子群为 $\{(1)\}$，A_3，S_3。因此 S_3 只有 1 个真正规子群，就是由偶置换全体组成的 A_3，相应的因子群为 $S_3/A_3\cong Z_2$。S_3 有子群格



其中 $H_1=\{(1),(12)\}$，$H_2=\{(1),(13)\}$，$H_3=\{(1),(23)\}$。

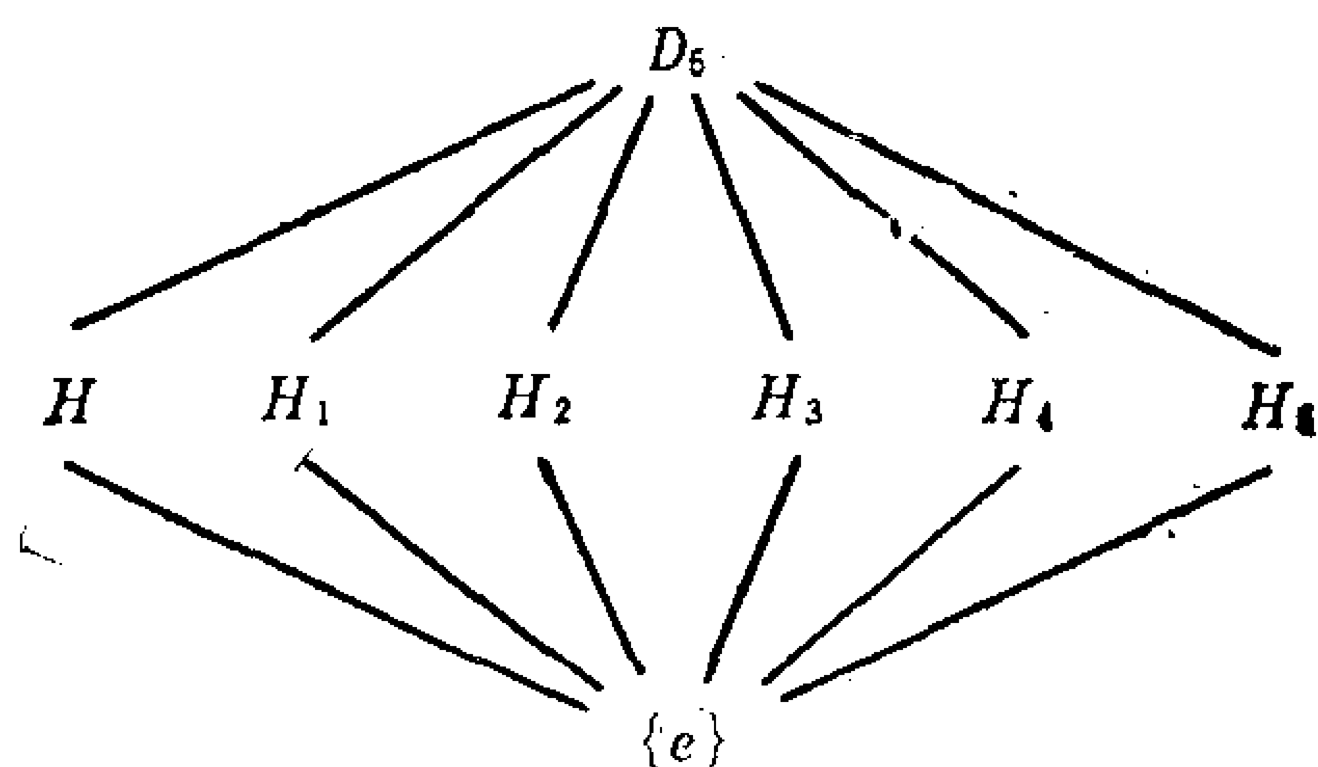
3.3.3.2　10 阶非阿贝尔群 G 同构于 D_5，D_5 有表现

$$D_5=\{a,\ b\mid a^5=b^2=1,\ bab^{-1}=a^4\}。$$

由于同构的群有完全相同的结构。下边对 D_5 进行讨论。D_5 的元素及相应元素的阶数见下表：

元素	e	a	a^2	a^3	a^4	b	ab	a^2b	a^3b	a^4b
阶数	1	5	5	5	5	2	2	2	2	2

通过计算，不难得到其共轭类是$\{e\}$，$\{a, a^4\}$，$\{a^2, a^3\}$，$\{b, a^2b, a^3b, a^4b\}$。在求共轭类时，注意共轭元有相同阶这一事实。D_5的中心$C(D_5)=\{e\}$，这由共轭类的结果或者D_5的定义关系均可得到。根据西洛定理，西洛5-子群就是5阶子群。5阶子群的个数$N(5)$具有性质$N(5)=1+5k$，其中k是非负整数，而且$N(5)|10$，因此$N(5)=1$，即只有1个5阶子群H，它是正规子群。不难看出，$H=\{e, a, a^2, a^3, a^4\}\cong Z_5$。西洛2-子群是2阶子群，2阶子群的个数$N(2)=1+2k$，其中$k$是非负整数，而且$1+2k|10$，于是$k$为0或2。如果$k=0$，则$N(2)=1$，存在2阶正规子群。但是，每个2阶元生成的2阶子群都不是正规子群。因此，只可能有$k=2$，$N(2)=5$。这5个2阶子群显然分别由5个2阶元生成，它们是$H_1=\langle b\rangle$，$H_2=\langle ab\rangle$，$H_3=\langle a^2b\rangle$，$H_4=\langle a^3b\rangle$，$H_5=\langle a^4b\rangle$。唯一的正规子群是$H=\langle a\rangle$，没有其它的真子群。D_5的子群格是



D_5的中心$C(D_5)=\{e\}$。考虑因子群G/H，由于$|G/H|=2$，$G/H\cong Z_2$是阿贝尔群，而且$H\supset G'=[G, G]$。熟知$G'\lhd G$，因此$G'=H$，或者$G'=\{e\}$。但是G是非阿贝尔群，因此$G'\neq\{e\}$，于是G的换位子群$G'=H$。

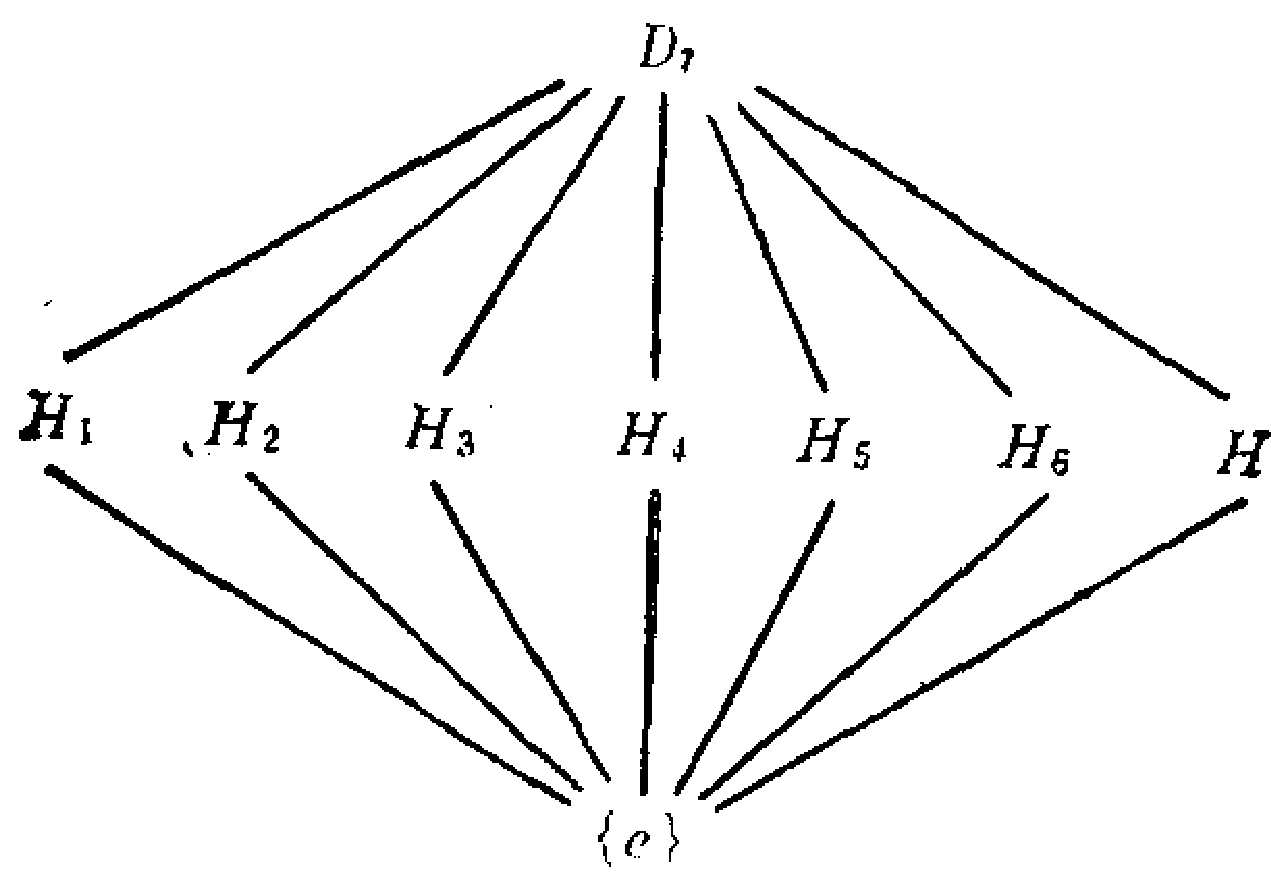
3.3.3.3　14阶非阿贝尔群G同构于D_7。D_7有表现

$$D_7=\{a, b \mid a^7=b^2=1, bab^{-1}=a^6\}。$$

D_7的元素与相应元素的阶数见下表：

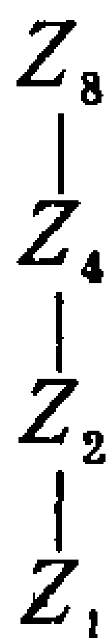
元素	e	a	a^2	a^3	a^4	a^5	a^6	b	ab	a^2b	a^3b	a^4b	a^5b	a^6b
阶数	1	7	7	7	7	7	7	2	2	2	2	2	2	2

其共轭类是$\{e\}$，$\{a, a^6\}$，$\{a^2, a^5\}$，$\{a^3, a^4\}$，$\{b, ab, a^2b, a^3b, a^4b, a^5b, a^6b\}$。$D_7$ 的中心 $C(D_7)=\{e\}$。D_7 有 7 个 2 阶子群，即 $H_1=\langle b\rangle$，$H_2=\langle ab\rangle$，$H_3=\langle a^2b\rangle$，$H_4=\langle a^3b\rangle$，$H_5=\langle a^4b\rangle$，$H_6=\langle a^5b\rangle$，$H_7=\langle a^6b\rangle$；有 1 个 7 阶子群 $H=\langle a\rangle$。H 是 D_7 的正规子群，$H\lhd D_7$，所以 $H=[D_7, D_7]=D_7'$。D_7 的唯一的非平凡因子群是 $D_7/H\cong Z_2$。D_7 的子群格为

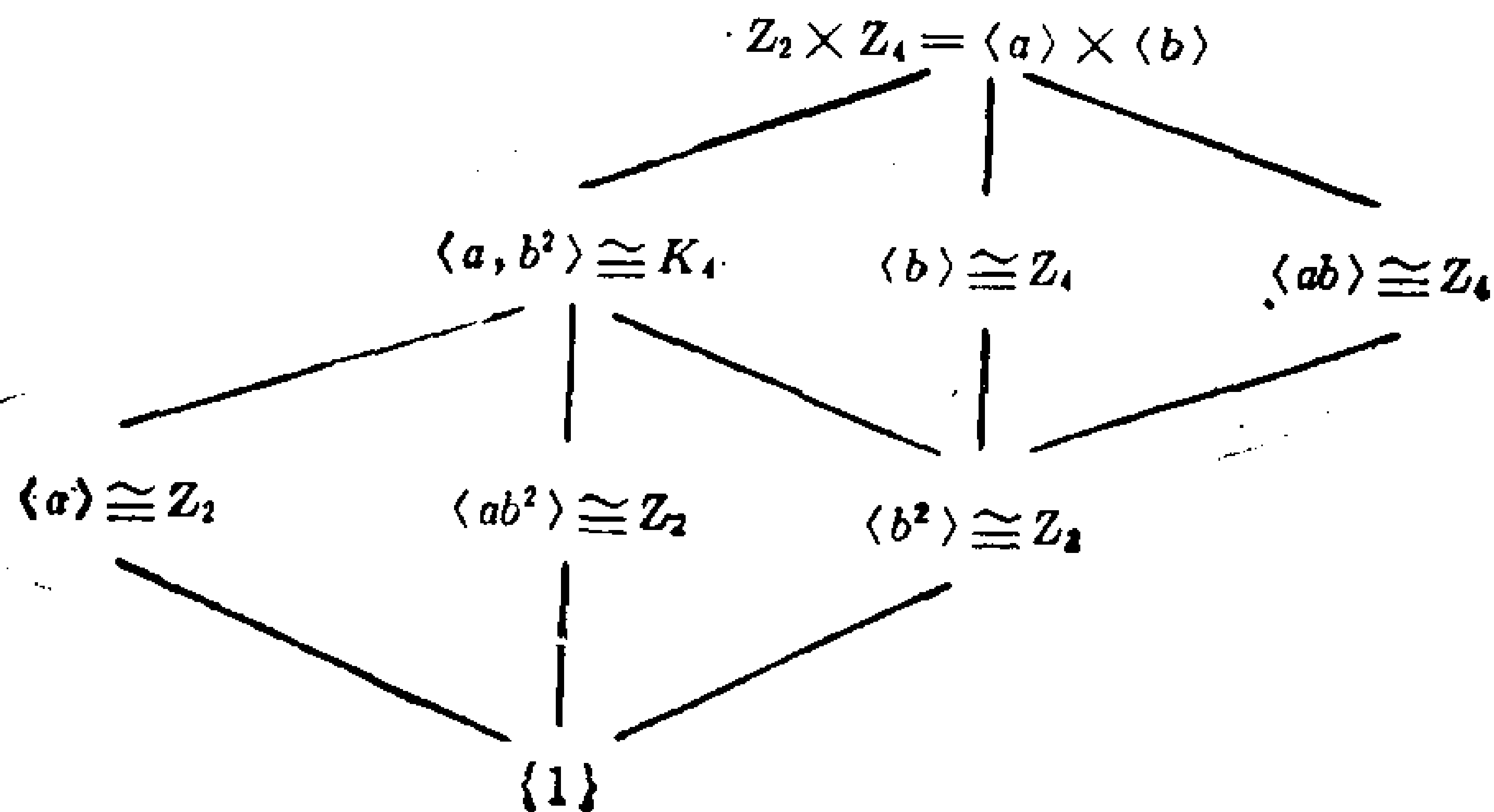


3.3.4 由定理 3.3.2，15 阶群只有循环群 Z_{15}。

于是只剩下阶数为 8 阶和 12 阶两种情形。8 阶阿贝尔群有 3 种：Z_8，$Z_4\times Z_2$，$Z_2\times Z_2\times Z_2$。Z_8 的子群格为

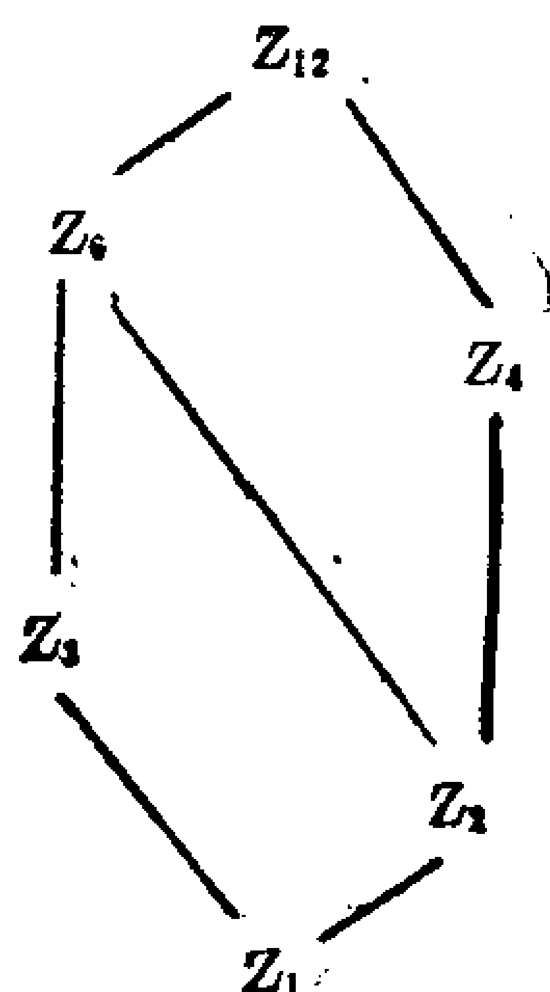


若令 $Z_2=\langle a\rangle$，$Z_4=\langle b\rangle$，其中 $a^2=b^4=1$，则 $Z_2\times Z_4$ 的子群格为

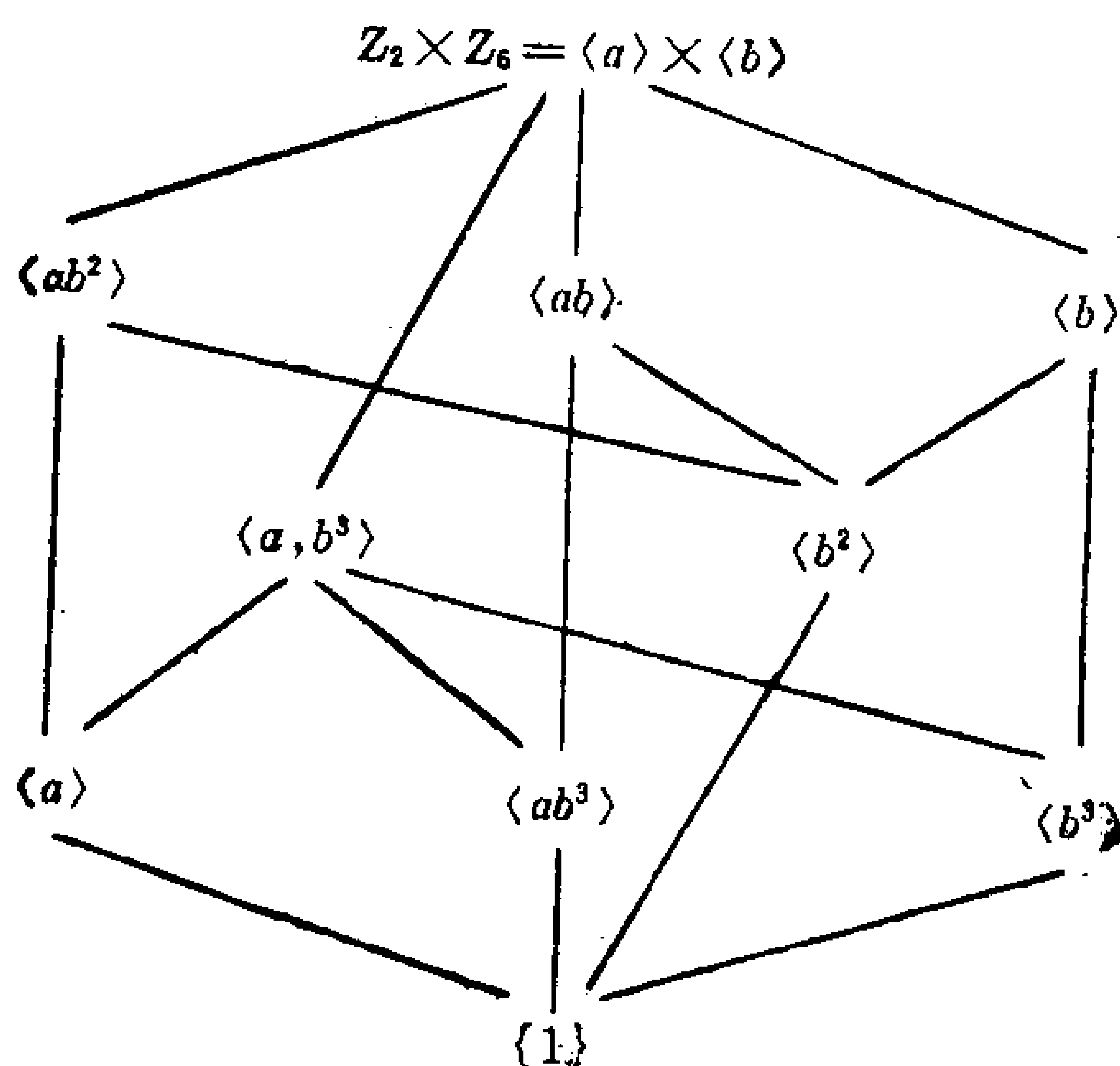


$Z_2\times Z_2\times Z_2$ 的子群格，作为练习，请读者自己给出。

12 阶阿贝尔群有 2 种：Z_{12} 和 $Z_2\times Z_6$。Z_{12} 的子群格为



若令 $Z_2\times Z_6=\langle a\rangle\times\langle b\rangle$，其中 $a^2=b^6=1$，则 $Z_2\times Z_6$ 的子群格为



易见，$Z_2\times Z_6$ 有 3 个 6 阶子群，即$\langle ab^2\rangle$，$\langle ab\rangle$，$\langle b\rangle$；1 个 4 阶子群$\langle a, b^3\rangle\cong K_4$，1 个 3 阶子群 $\langle b^2\rangle$ 和 3 个 2 阶子群 $\langle a\rangle$，$\langle ab^3\rangle$，$\langle b^3\rangle$。8 阶和 12 阶非阿贝尔群的讨论较为复杂，见下面的定理。

定理3.3.3 8 阶非阿贝尔群G只有 2 个，即为 D_4 和 Q_8。D_4 的表现是

$$D_4=\langle a, b\mid a^4=b^2=(ba)^2=1\rangle,$$

Q_8 的表现是

$$Q_8=\langle a,\ b\,|a^4=1,\ b^2=a^2,\ ba=a^3b\rangle。$$

证明 如果G有8阶元素，则G为循环群。如果G中每个非单位元素$a(\neq 1)$的阶均为2，则G是阿贝尔群。若G为非阿贝尔群，则G中必有4阶元素a。由于$[G:\langle a\rangle]=2$，从而$\langle a\rangle$是G的正规子群。取$b\notin\langle a\rangle$，则G由a和b生成并且$b^2\in\langle a\rangle$。令$b^2=a^i(0\leqslant i\leqslant 3)$，由于$b$的阶$\leqslant 4$，从而$b^2$的阶$\leqslant 2$。因此$i\neq 1,\ 3$，即$b^2=1$或者$b^2=a^2$。

如果$b^2=1$，由于$\langle a\rangle$为正规子群，从而$bab^{-1}=a^i(0\leqslant i\leqslant 3)$。因为$bab^{-1}$的阶等于$a$的阶，即阶为4，从而$i=1$或3。如果$bab^{-1}=a$，则$ba=ab$，从而$G$为阿贝尔群。所以$bab^{-1}=a^3=a^{-1}$，于是$G=\langle a,\ b\,|a^4=b^2=1,\ ba=a^{-1}b\rangle=D_4$。

如果$b^2=a^2$，则与前同样有$bab^{-1}=a^3$，于是$G=\langle a,b\,|a^4=1,\ b^2=a^2,\ ba=a^{-1}b\rangle=Q_8$。

最后还要证明D_4和Q_8不同构。这可以考查两个群中元素的阶。这两个群中8个元素均表成$a^ib^j(0\leqslant i\leqslant 3,\ 0\leqslant j\leqslant 1)$，但是乘法运算不同，不难计算它们的阶分别为：

群D_4:

元素	1	a	a^2	a^3	b	ab	a^2b	a^3b
阶数	1	4	2	4	2	2	2	2

群Q_8:

元素	1	a	a^2	a^3	b	ab	a^2b	a^3b
阶数	1	4	2	4	4	4	4	4

由于两个群中4阶元素的个数不同，所以D_4和Q_8不同构。证毕。

练习3.3.1 求证$C(D_4)=\{1\}$，$C(Q_8)=\{1,\ a^2\}$。

定理3.3.4 12阶非阿贝尔群G有三个，即D_6，A_4和$T=\langle a,\ b\,|a^6=1,\ b^2=a^3,\ ba=a^{-1}b\rangle$。

证明 取G的一个3阶西洛子群$P=\langle c\rangle$，G作用在对子集

P的陪集上给出诱导表示$f: G\to S_4$（$4=[G:P]$）。$K=\mathrm{Ker}f\leqslant P$，于是$K=P$或者$\{1\}$。

如果$K=\{1\}$，则$f: G\to S_4$为单同态，从而$[S_4: f(G)]=\frac{24}{12}=2$。但是$S_4$的12阶子群只有$A_4$，于是这时$G\cong A_4$。

当$K=P$时，$P\lhd G$，从而G只有唯一的3阶子群P，因此G只有两个3阶元素c和c^2。由于$[G:C_G(c)]$等于c之共轭元个数，从而$[G:C_G(c)]=1$或2，$|C_G(c)|=12$或6，$C_G(c)$中必有2阶元素d。令$a=cd=dc$，则a是6阶元素，所以$\langle a\rangle$为G的正规子群。

取$b\notin\langle a\rangle$，则$b\neq 1$，而$bab^{-1}=a^i$（$0\leqslant i\leqslant 5$）。由于bab^{-1}为6阶元素，所以$i=\pm 1$。由于$i=1$时，$ba=ab$，而G为阿贝尔群，从而必然$bab^{-1}=a^{-1}$，即$ba=a^{-1}b$。

再由$b^2\in\langle a\rangle$，从而$b^2=a^j$（$D\leqslant j\leqslant 5$），于是$a^j=b^2=ba^jb^{-1}=(bab^{-1})^j=a^{-j}$，$a^{2j}=1$，从而$j=0$或$3$。

当$j=0$时，$b^2=1$，从而$G=\langle a, b\,|a^6=b^2=1, ba=a^{-1}b\rangle=D_6$。

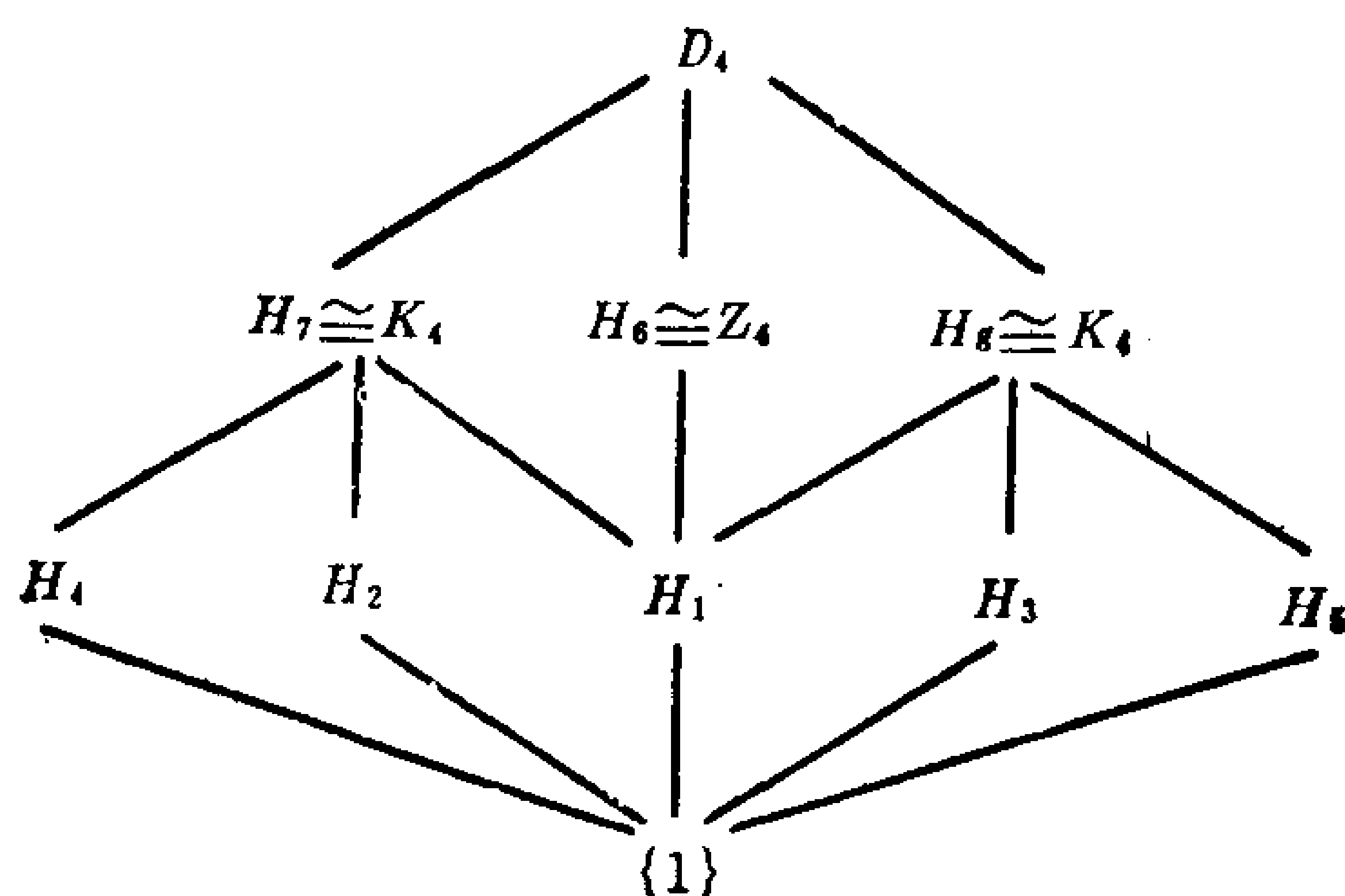
当$j=3$时，$G=\langle a, b\,|a^6=1, b^2=a^3, ba=a^{-1}b\rangle=T$。

现证明$T=\langle a, b\,|a^6=1, b^2=a^3, ba=a^{-1}b\rangle$是12阶群。首先，$T$中元素均可写成$a^ib^j$（$0\leqslant i\leqslant 5$，$0\leqslant j\leqslant 1$），从而$|T|\leqslant 12$。其次考虑群$S_3\times Z_4$中元素$A=((123), \alpha^2)$，$B=((12), \alpha)$，其中$Z_4=\langle\alpha\,|\alpha^4=1\rangle$则$A^6=1$，$B^2=A^3$，$BA=A^{-1}B$，直接验证$A$和$B$生成12阶群。由此可知$T$是12阶群。

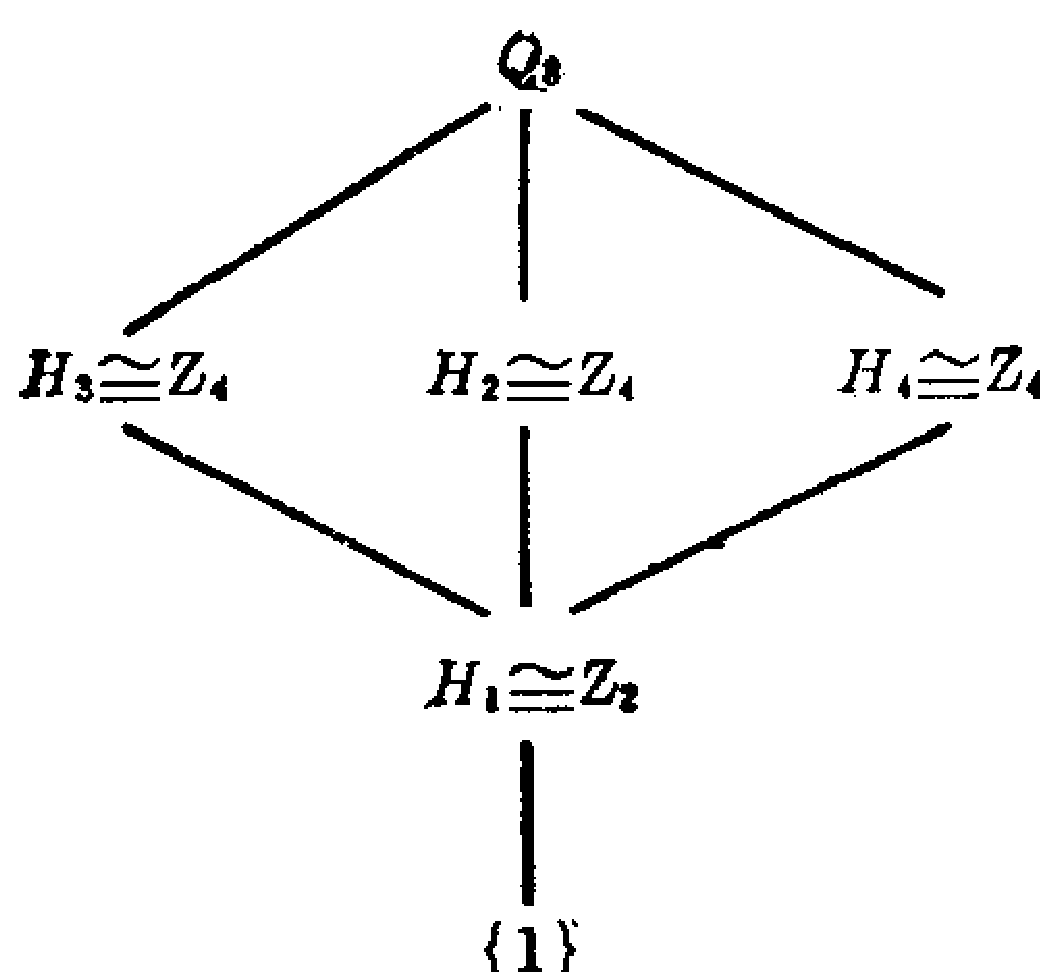
最后还需证明D_6，A_4和T彼此不同构。首先，T中有4阶元素b，而D_6和A_4均没有4阶元素，从而T与D_6或A_4不同构。其次，D_6中有7个二阶元素：a^3，a^ib（$0\leqslant i\leqslant 5$），而A_4中只有3个二阶元素$(12)(34)$，$(13)(24)$，$(14)(23)$。从而D_6与A_4也不同构。证毕。

3.3.5 由定理3.3.3已知，8阶非阿贝尔群是D_4或Q_8，进而有：

3.3.5.1 D_4 的共轭类为 $\{1\}$，$\{a^2\}$，$\{a, a^3\}$，$\{b, a^2b\}$，$\{ab, a^3b\}$，中心 $C(D_4)=\{1, a^2\}$，换位子群 $D'_4=\{1, a^2\}$。真子群的阶只可能是 2 或 4，因此 D_4 的 2 阶子群为 $H_1=\langle a^2\rangle$，$H_2=\langle b\rangle$，$H_3=\langle ab\rangle$，$H_4=\langle a^2b\rangle$，$H_5=\langle a^3b\rangle$。由于 $H_1=D'_4$，$H_1\triangleleft G$。正规子群必包有完全共轭类，即若含有某个共轭类中的 1 个元素，则必含有此共轭类中的每一个元素。因此，H_2, H_3，H_4，H_5 都不是正规子群。4 阶子群只可能是 Z_4 或者 K_4，不难看出 D_4 的 4 阶子群为 $H_6=\langle a\,|a^4=1\rangle$，$H_7=\langle a^2, b\,|a^2b=ba^2\rangle\cong K_4$，$H_8=\langle a^2, ab|a^3b=aba^2\rangle\cong K_4$。由于 $[D_4:H_6]=[D_4:H_7]=[D_4:H_8]=2$，因此 $H_6\triangleleft D_4$，$H_7\triangleleft D_4$，$H_8\triangleleft D_4$。D_4 的因子群 $D_4/H_6\cong D_4/H_7\cong D_4/H_8\cong Z_2$，$D_4/D'_4\cong K_4$。综合上述，$D_4$ 的子群格为



3.3.5.2 Q_8 的共轭类为 $\{1\}$，$\{a^2\}$，$\{a, a^3\}$，$\{b, a^2b\}$，$\{ab, a^3b\}$，Q_8 的中心 $C(Q_8)=\{1, a^2\}=\langle a^2\rangle$，换位子群 $Q'_8=[Q_8, Q_8]=C(Q)$。2 阶子群只有 1 个 $H_1=\langle a^2\rangle$。由于 Q_8 只有 1 个 2 阶元，因此 4 阶子群只可能是循环群，故 4 阶子群为 $H_2=\langle a\rangle$，$H_3=\langle b\rangle$，$H_4=\langle ab\rangle$，它们都是正规子群，即 $H_i\triangleleft Q_8$（$i=2, 3, 4$）。Q_8 的因子群是 $Q/H_2\cong Q/H_3\cong Q/H_4\cong Z_2$，$Q/H_1\cong K_4$。$Q_8$ 的子群格为



Q_8 的所有真子群都是正规的和循环的。

3.3.6 由定理3.3.4，12阶非阿贝尔群G有3种：

$$D_6=\langle a,\ b\,|a^2=b^6=1,(ba)^2=1\rangle,$$

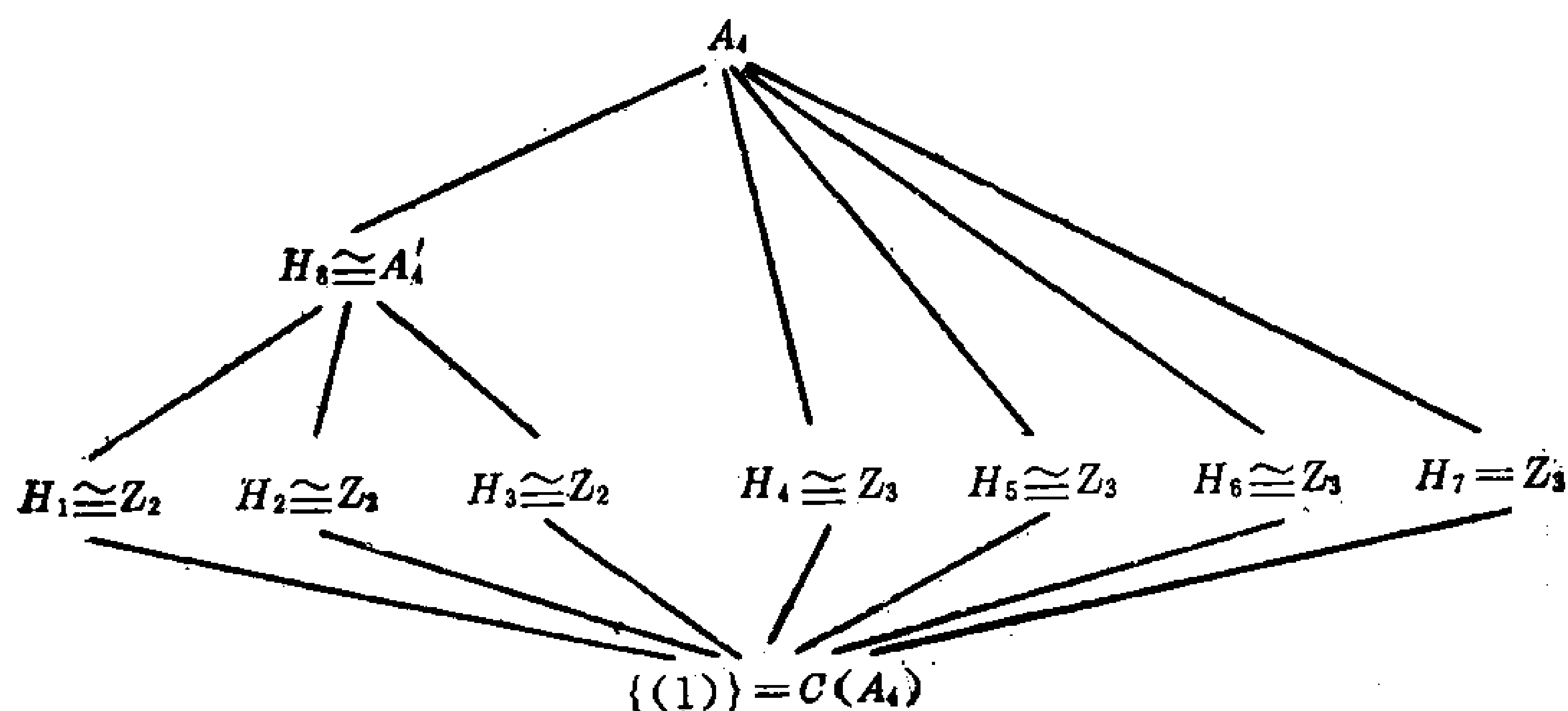
$$A_4=\langle a=(12)(34),\ b=(123)|a^2=b^3=1,(ba)^3=1\rangle,$$

$$T=\langle a,\ b\,|a^6=1,\ b^2=a^3,\ ba=a^{-1}b\rangle。$$

3.3.6.1 D_6 的共轭类为$\{1\}$，$\{b^3\}$，$\{b^2,\ b^4\}$，$\{b,\ b^5\}$，$\{a,\ ab^2,\ ab^4\}$，$\{ab,\ ab^3,\ ab^5\}$，D_6 的中心$C(D_6)=\langle b^3\rangle\cong Z_2$，换位子群 $D_6'=\langle b^2\rangle\cong Z_3$。2阶子群为 $H_1=\langle a\rangle$, $H_2=\langle b^3\rangle$, $H_3=\langle ab\rangle$，$H_4=\langle ab^2\rangle$，$H_5=\langle ab^3\rangle$，$H_6=\langle ab^4\rangle$，$H_7=\langle ab^5\rangle$，它们都同构于 Z_2。3阶子群只有1个 $H_8=\langle b^2\rangle=D_6'$。4阶子群有3个，它们是$H_9=\langle a,\ b^3|ab^3=b^3a\rangle\cong K_4$，$H_{10}=\langle b^3, ab^2|b^3\cdot ab^2=ab^2\cdot b^3\rangle\cong K_4$；$H_{11}=\langle b^3,\ ab|b^3ab=ab^4\rangle\cong K_4$。6阶子群有3个，它们是 $H_{12}=\langle b\rangle\cong Z_6$，$H_{13}=\langle a,\ b^2|(b^2a)^2=1\rangle\cong S_3$，$H_{14}=\langle b^2,\ ab^3|(b^2ab^3)^2=1\rangle\cong S_3$。其中$C(D_6)=H_2$，$D_6'=H_8$，$H_{12}$，$H_{13}$，$H_{14}$ 是 D_6 的真正规子群。相应的因子群为 $D_6/C(D_6)\cong S_3$，$D_6/D_6'\cong K_4$，$D_6/H_{12}\cong D_6/H_{13}\cong D_6/H_{14}\cong Z_2$。进而，$H_2\cap H_{13}=\{1\}$，$D_6\cong H_2\times H_{13}\cong Z_2\times S_3\simeq Z_2\times D_3$。请读者自己画出 D_6 的子群格图。

3.3.6.2 A_4 的共轭类为 $\{(1)\}$，$\{(12)(34),\ (13)(24),\ (14)(23)\}$，$\{(123), (142), (134), (243)\}$，$\{(132), (124), (143),$

(234)}。A_4的中心是只有1个元素的共轭类的并，因此$C(A_4)=\{(1)\}$。A_4没有2阶正规子群和6阶子群。换位子群A_4'的阶只可能为3，4，或者12。根据西洛定理，A_4有4个3阶子群，因此A_4'的阶不可能是3。易知，$K_4=\{(1),(12)(34),(13)(24),(14)(23)\}$是$A_4$的正规子群，即$K_4 \lhd A_4$，和$A_4/K_4 \cong Z_3$是阿贝尔群。于是$A_4' \subset K_4$，得到$A_4'=K_4$。$A_4$的2阶子群均由2阶元素生成，它们是$H_1=\langle(12)(34)\rangle$，$H_2=\langle(13)(24)\rangle$，$H_3=\langle(14)(23)\rangle$。3阶子群为$H_4=\langle(123)\rangle$，$H_5=\langle(243)\rangle$，$H_6=\langle(134)\rangle$，$H_7=\langle(142)\rangle$。只有1个4阶子群$H_8=A_4'=K_4$。$A_4$的子群格是



由于A_4'是A_4的唯一的真正规子群，因此唯一的非平凡商子群是$A_4/A_4' \cong Z_3$。

练习3.3.2 证明A_4没有6阶子群，也没有2阶正规子群。

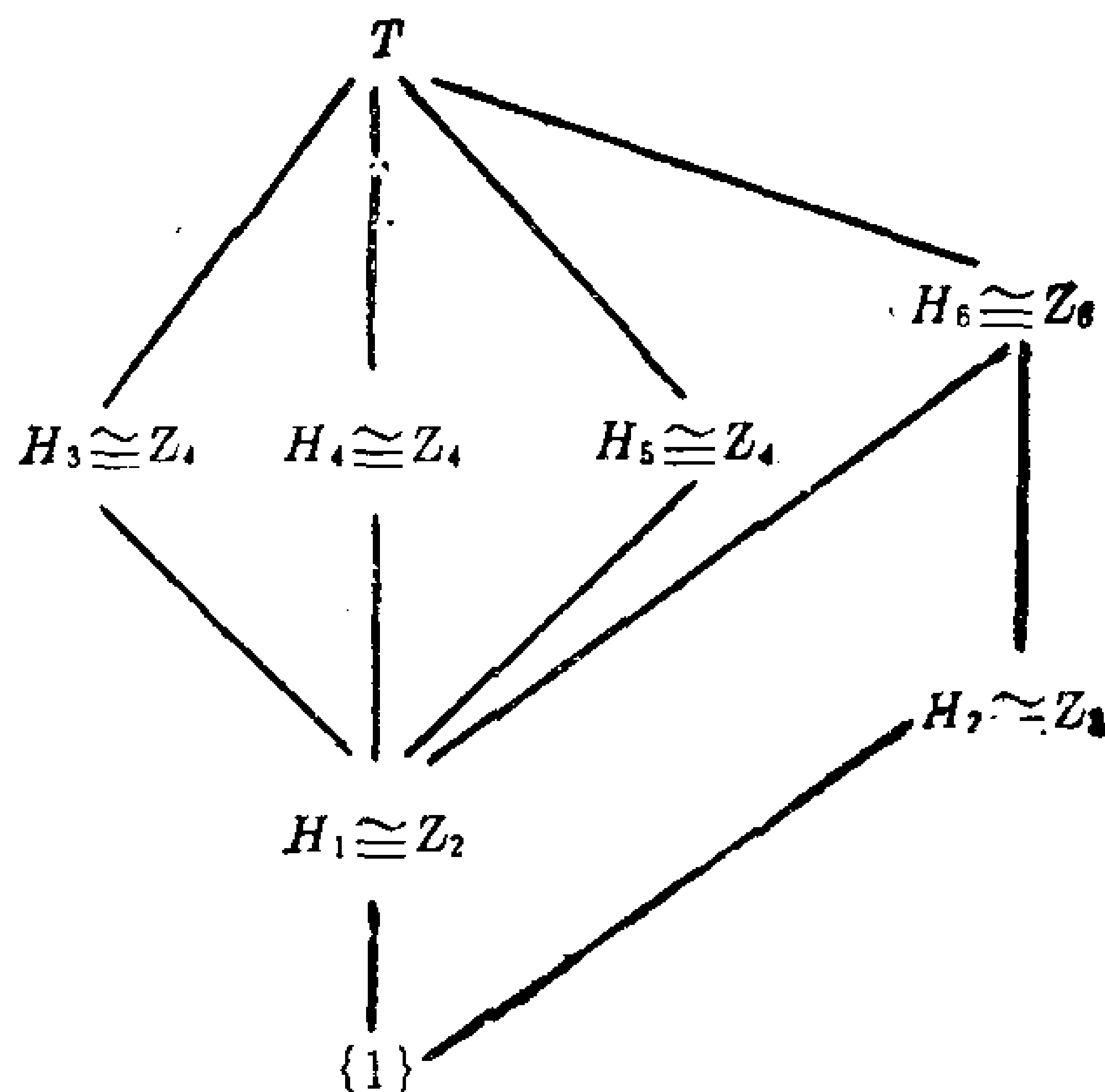
3.3.6.3 为方便起见，给出T的另一个表现

$$T=\langle c, d \mid c^4=d^3=1, dc=cd^2\rangle,$$

其中$c=a^2b$，$d=a^2$，$a=d^2c^2$，$b=c$。T的元素和相应的阶数为

元素	1	d	d^2	c	cd	cd^2	c^2	c^2d	c^2d^2	c^3	c^3d	c^3d^2
阶数	1	3	3	4	4	4	2	6	6	4	4	4

共轭类为$\{1\}$，$\{c^2\}$，$\{d, d^2\}$，$\{c^2d, c^2d^2\}$，$\{c, cd, cd^2\}$，$\{c^3, c^3d, c^3d^2\}$。中心$C(T)=\{1, c^2\}\cong Z_2$，换位子群$T'=\langle d\rangle\cong Z_3$。2阶子群只有一个$H_1=\langle c^2\rangle=C(T)$。由于3阶子群由3阶元素生成，因此3阶子群也只有一个$H_2=\langle d\rangle=T'$。利用西洛定理，T有3个4阶子群，它们是$H_3=\langle c\rangle\cong Z_4$，$H_4=\langle cd\rangle\cong Z_4$，$H_5=\langle cd^2\rangle\cong Z_4$，显然它们都不是正规子群。由于任何6阶子群在$T$中的指数都是2，因此是正规子群。再考虑到6阶子群不可能包有4阶元素，可得T只有1个6阶子群$H_6=\{1, d, d^2, c^2, c^2d, c^2d^2\}=\langle c^2d\rangle\cong Z_6$，$H_6\lhd T$。$T$的所有真子群都是循环群。$T$的子群格为



T的非平凡因子群为$T/C(T)\cong S_3$，$T/T'\cong Z_4$，$T/H_6\cong Z_2$。

练习3.3.3 令$c_1=\begin{pmatrix}0 & i\\ i & 0\end{pmatrix}$，$d_1=\begin{pmatrix}\omega & 0\\ 0 & \omega^2\end{pmatrix}$，其中$i^2=-1$，$\omega=-\frac{1}{2}+i\frac{\sqrt{3}}{2}$，求证$c_1$，$d_1$在复数域$\mathbb{C}$上的2阶一般线性群$GL_2(\mathbb{C})$中生成的子群$\langle c_1, d_1\rangle$同构于$T$。

练习3.3.4 证明$T/C(T)\cong S_3$，$T/T'\cong Z_4$。

1 到 15阶 群群表

阶数	个数	阿　贝　尔　型	个数	非阿贝尔型
1	1	$\{1\}$	0	—
2	1	Z_2	0	—
3	1	Z_3	0	—
4	2	Z_4 $K_4=Z_2\times Z_2$	0	—
5	1	Z_5	0	—
6	1	$Z_6=Z_2\times Z_3$	1	$S_3=D_3$
7	1	Z_7	0	—
8	3	Z_8, $Z_4\times Z_2$, $Z_2\times Z_2\times Z_2$	2	D_4, Q_8
9	2	Z_9, $Z_3\times Z_3$	0	—
10	1	$Z_{10}=Z_2\times Z_5$	1	D_5
11	1	Z_{11}	0	—
12	2	$Z_{12}=Z_3\times Z_4$, $Z_3\times K_4$	3	A_4, T, $D_6=Z_2\times D_3$
13	1	Z_{13}	0	—
14	1	$Z_{14}=Z_2\times Z_7$	1	D_7
15	1	$Z_{15}=Z_3\times Z_5$	0	—

§3.4　幂零群和可解群

设G为群，则G的中心$C_1(G)=C(G)$为G的正规子群。令$C_2(G)$是正则满同态$G\to G/C_1(G)$之下$C(G/C_1(G))$的原像，于是$C_2(G)\lhd G$。一般地，令$C_n(G)$是正则满同态$G\to G/C_{n-1}(G)$之下$C(G/C_{n-1}(G))$的原像，于是我们有正规子群列

$$\{1\}\leqslant C_1(G)\leqslant C_2(G)\leqslant\cdots, C_n(G)\lhd G$$

这叫G的**中心升列**。

定义 3.4.1 群G叫**幂零群**，是指存在$n \geqslant 1$，使得$C_n(G) = G$。

例 3.4.1 每个阿贝尔群均是幂零的，因为$C_1(G) = C(G) = G$。

例 3.4.2 每个有限p-群G（即有限群G中每个元素的阶均是p的方幂）均是幂零的，这是因为若$G \neq 1$，则有限p-群G有非平凡中心，即$C(G) \neq \{1\}$。而当$G \neq C_i(G)$时，$C_i(G)$是$C_{i+1}(G)$的真子群。由于G为有限群，从而必然有n使$C_n(G) = G$。

例 3.4.3 有限多个幂零群的直积也是幂零群。

证明　不妨设$G = H \times K$（对于多个因子的情形可以归纳证明），可以归纳证明$C_i(G) = C_i(H) \times C_i(K)$（对每个$i \geqslant 1$）。如果$H$和$K$均为幂零群，则有$n$，$m \geqslant 1$，使$C_n(H) = H$，$C_m(K) = K$。取$l = \max(n, m)$，则$C_l(G) = C_l(H) \times C_l(K) = H \times K = G$。即$G$为幂零群。

引理 3.4.1 如果H是幂零群G的真子群，则H也是$N_G(H)$的真子群。

证明　令$C_0(G) = \{1\}$设n为最大下标，使得$C_n(G) \leqslant H$（由于G幂零而H是G的真子群，这样的n是存在的）。取$a \in C_{n+1}(G)$，$a \notin H$，则对每个$h \in H$。在$G/C_n(G)$中，$C_nah = (C_na)(C_nh) = (C_nh)(C_na) = C_nha$（因由$C_{n+1}(a)$的定义知$C_na$在$G/C_n(G)$的中心之中）。于是，$ah = h'ha, h' \in C_n(G) \leqslant H$。从而$aha^{-1} \in H$，即$a \in N_G(H)$。但是$a \notin H$，从而$H$为$N_G(H)$的真子群。证毕。

定理 3.4.1 有限群G是幂零群，当且仅当G是它的西洛子群的直积。

证明　设G为它的西洛子群的直积。由于每个西洛子群均为p-群，由例 3.4.2 和例 3.4.3知G为幂零群。反之，设G为幂零群。对于$|G|$的每个素因子p，令P为G的一个西洛p-子群。如果$P = G$，则证毕。如果P为G的真子群，由引理 3.4.1

可知P为$N_G(P)$的真子群。但是$N_G(P)=N_G(N_G(P))$（记$N=N_G(P)$，则$P\lhd N$，从而P是N中唯一的西洛p-子群。于是$x\in N_G(N)\Rightarrow xNx^{-1}=N\Rightarrow xPx^{-1}\leqslant N\Rightarrow xPx^{-1}=P\Rightarrow x\in N$，从而$N_G(N)=N$）。由引理3.4.1可知，$N_G(P)=G$，从而$P\lhd G$，即$P$是$G$中唯一的西洛$p$-子群。

设$|G|=p_1^{\lambda_1}\cdots p_k^{\lambda_k}$，令$P_i$是$G$中唯一的西洛$p_i$-子群，则$|P_i|=p_i^{\lambda_i}(1\leqslant i\leqslant k)$，$P_i\lhd G$，并且$P_i\cap P_j=\{1\}(i\neq j$时)。从而当$i\neq j$时，$P_i$中元素和$P_j$中元素可交换，因此$P_1P_2\cdots P_{m-1}$中元素的阶均是$p_1^{\lambda_1}\cdots p_{m-1}^{\lambda_{m-1}}$的因子，从而$P_1P_2\cdots P_{m-1}\cap P_m=\{1\}(2\leqslant m\leqslant k)$，表明$G=P_1\cdots P_k=P_1\times\cdots\times P_k$。证毕。

系 3.4.1 设G为幂零有限群，则对于$|G|$的每个因子m，G均有m阶子群。

证明 如前设$G=p_1^{\lambda_1}\cdots p_k^{\lambda_k}$，则$G=P_1\times\cdots\times P_k$，$|P_i|=p_i^{\lambda_i}$。如果$m\,||G|$，则$m=p_1^{\mu_1}\cdots p_k^{\mu_k}$，$\mu_i\leqslant\lambda_i$。根据西洛理论，$P_i$有$p_i^{\mu_i}$阶子群$Q_i$。从而子群$Q_1\times\cdots\times Q_k$即为所求。

系 3.4.2 幂零有限群G的子群和商群均是幂零群。

证明 如上设$G=P_1\times\cdots\times P_k$，$P_i$为$G$中唯一的西洛$p_i$-子群。如果$H\leqslant G$，令$Q_i$为$H$的一个西洛$p_i$-子群。由西洛理论$Q_i\leqslant P_i(1\leqslant i\leqslant k)$，从而必然$H=Q_1\times\cdots\times Q_k$，即$H$为幂零群。如果$H\lhd G$，则$Q_i\lhd P_i$，而$G/H\cong P_1/Q_1\times\cdots\times P_k/Q_k$。易知，$P_i/Q_i$为$G/H$的西洛$p_i$-群。所以$G/H$也是幂零群。证毕。

现在介绍可解群。设G为群，对于a、$b\in G$，元素$[a,b]=aba^{-1}b^{-1}$叫作a和b的**换位子**。所有换位子生成的群G'叫作G的**换位子群**。易知，G为阿贝尔群$\Longleftrightarrow G'=\{1\}$。从而在某种意义下，可用$G'$来衡量$G$与阿贝尔群相距多远。

定理 3.4.2 （1）$G'\lhd G$；

（2）若$N\lhd G$，则G/N为阿贝尔群$\Longleftrightarrow G'\leqslant N$。

证明（1）对于g，a，$b\in G$，易知$g[a,b]g^{-1}=[gag^{-1},gbg^{-1}]$，从而$gG'g^{-1}=G'$，即$G'\lhd G$。

（2）若G/N为阿贝尔群，则对每个a，$b\in G$，$abN=$

baN。于是$[a, b]=aba^{-1}b^{-1}\in N$，即$G'\leqslant N$。反之，若$G'\leqslant N$，则$G/N\cong\frac{G/G'}{N/G'}$。从而$G/N$同构于阿贝尔群$G/G'$的商群，因此$G/N$也为阿贝尔群。证毕。

记$G^{(1)}=G'$，$G^{(i)}=G^{(i-1)\prime}$ ($i\geqslant 2$)，称$G^{(i)}$为G的第i导出子群。由此给出正规子群列

$$G\geqslant G^{(1)}\geqslant G^{(2)}\geqslant\cdots,\quad G^{(i)}\lhd G^{(i-1)}.$$

练习 3.4.1 证明$G^{(i)}\lhd G$（对每个i）。

定义 3.4.2 群G叫作**可解群**，是指有$n\geqslant 1$，使得$G^{(n)}=\{1\}$。

每个阿贝尔群都可解。更一般地有如下定理。

定理 3.4.3 幂零群必为可解群。

证明 由定义知$C_i(G)/C_{i-1}(G)=C(G/C_{i-1}(G))$为阿贝尔群，从而当$i\geqslant 2$时，$C_i(G)'\leqslant C_{i-1}(G)$（定理 3.4.2），$C_1(G)'=C(G)'=\{1\}$。如果$G$为幂零群，则有$n$使得$G=C_n(G)$。于是$C(G/C_{n-1}(G))=C_n(G)/C_{n-1}(G)=G/C_{n-1}(G)$，从而$G^{(1)}=G'\leqslant C_{n-1}(G)$，$G^{(2)}=G^{(1)\prime}\leqslant C_{n-1}(G)'\leqslant C_{n-2}(G)$。类似地，$G^{(3)}\leqslant C_{n-2}(G)'\leqslant C_{n+3}(G)$，…，$G^{(n)}\leqslant C_1(G)'=\{1\}$，即$G^{(n)}=\{1\}$。从而$G$为可解的。

定理 3.4.4 （1）可解群的子群和商群均可解。

（2）如果$N\lhd G$，则G可解$\Longleftrightarrow N$和G/N均可解。

证明 （1）设G是可解群，f：$G\to H$为群的同态。易知$f(G^{(i)})\leqslant H^{(i)}$，并且若$f(G)=H$，则$f(G^{(i)})=H^{(i)}$。由此即知，$G$的每个子群和商群均可解。

（2）$\Rightarrow$由（1）推得。反之，设G/N和N均可解，考虑正则满同态f：$G\to G/N$，由G/N的可解性知，有n使$f(G^{(n)})=(G/N)^{(n)}=\{1\}$，于是$G^{(n)}\leqslant N$。由$N$可解知，$G^{(n)}$也可解。从而有$m$使$(G^{(n)})^{(m)}=\{1\}$，即$G^{(n+m)}=\{1\}$，于是$G$可解。

练习 3.4.2 设$N\lhd G$，如果N和G/N均为幂零群，G是

否为幂零群？（提示：考虑 S_3。）

下面给出一组不可解群的例子。

系 3.4.2 $n \geq 5$ 时，S_n 为不可解群。

证明 若 S_n 可解，则子群 A_n 也可解。因为 A_n 不是阿贝尔群，从而 $A'_n \neq \{1\}$。但是，$A'_n \lhd A_n$，而 A_n 又为单群（当 $n \geq 5$ 时），于是 $A'_n = A_n$。对所有 $i \geq 1$，$A_n^{(n)} = A_n \neq \{1\}$，从而 A_n 不可解。因此 S_n 也不可解。证毕。

利用域的伽罗瓦（Galois）理论，由系 3.4.2 可以推出，当 $n \geq 5$ 时，n 次一般代数方程 $x^n + a_1x^{n-1} + \cdots + a_n = 0$ 是根式不可解的（即没有一般求解公式）。

英国数学家伯恩赛德（Burnside）提出的伯恩赛德猜想：每个奇阶群均是可解群。这个猜想于 1963 年由费特（W. Feit）和汤姆森(J. Thompson）所证明。

练习 3.4.3 设 $H, K \leq G$，以 $[H, K]$ 表示由 $\{[h, k] \mid h \in H, k \in K\}$ 生成的 G 的子群。

(a) $[H, K] \lhd (H \cup K)$（右边 $(H \cup K)$ 表示 G 中由集合 $H \cup K$ 生成的子群）；

(b) $[H, G'] = \{1\} \Rightarrow [H', G] = \{1\}$；

(c) $H \lhd G \Longleftrightarrow [H, G] \leq H$；

(d) 设 $K \lhd G$，$K \leq H$，则 $H/K \leq C(G/K) \Longleftrightarrow [H, G] \leq K$。

练习 3.4.4 设 G 为群。定义 $\gamma_1(G) = G$，$\gamma_2(G) = [G, G]$，当 $n \geq 2$ 时 $\gamma_n(G) = [\gamma_{n-1}(G), G]$。求证：$G$ 为幂零群 $\Longleftrightarrow$ 存在 $n \geq 1$ 使得 $\gamma_n(G) = \{1\}$。

练习 3.4.5 G 为幂零群，$\{1\} \neq N \lhd G$，则 $N \cap C(G) \neq \{1\}$。

练习3.4.6 $D_n = \langle a、b \mid a^n = b^2 = 1, ba = a^{-1}b \rangle$ $(n \geq 3)$。

(a) $a^2 \in D'_n$；

(b) 若 n 为奇数，则 $D'_n \cong Z_n$，若 n 为偶数，则 $D'_n = Z_m$，$m = n/2$；

（c）D_n 为幂零群$\Longleftrightarrow n$ 为 2 的方幂。

练习3.4.7 （a）$S_4'=A_4$；

（b）S_3 和 S_4 为可解群，但不是幂零群。

从上面定义看出，幂零群和可解群分别与中心升列和导出群列有关。下面更一般地研究这种正规群列，并且给出可解群的另一种刻划形式（定理 3.4.5）。

定义3.4.3 设 $G=G_0\geqslant G_1\geqslant\cdots\geqslant G_n$ 是群G 的子群列。如果 $G_{i+1}\lhd G_i$（$0\leqslant i\leqslant n-1$），则叫作 G 的一个**正规群列**，商群 G_i/G_{i+1}均叫此正规群列的**因子**。其中非平凡因子的个数（即为列中$\geqslant$是 7 的个数）叫作此正规列的**长度**。

例如：导出列$G\geqslant G^{(1)}\geqslant G^{(2)}\geqslant\cdots\geqslant G^{(n)}$ 和中心升列$G=C_n(G)\geqslant C_{n-1}(G)\geqslant\cdots\geqslant C_1(G)$ 均为正规列。

定义3.4.4 设$G=G_0\geqslant G_1\geqslant\cdots\geqslant G_n$是$G$的正规列，则它的一个**一步加细**是指正规列 $G=G_0\geqslant G_1\geqslant\cdots\geqslant G_i\geqslant N\geqslant G_{i+1}\geqslant\cdots\geqslant G_n$（对某个 $0\leqslant i\leqslant n-1$），或者$G=G_0\geqslant G_1\geqslant\cdots\geqslant G_n\geqslant N_0$通过有限次一步加细得到的正规列叫原正规列的**加细**。如果加细序列的长度大于原来正规列，则称它为真加细。

定义3.4.5 正规列$G=G_0\geqslant G_1\geqslant\cdots\geqslant G_n=\{1\}$叫**组成列**，是指它的每个因子 G_i/G_{i+1} 均是单群。上述正规列叫可解列，是指每个因子 G_i/G_{i+1} 均是阿贝尔群。

以下经常要采用第一章中的以下结果：若$N\lhd G$，则G/N的每个正规子群均有形式H/N，其中$N\lhd H\lhd G$。从而当$G\neq N$时，G/N为单群$\Longleftrightarrow N$是G的**极大正规子群**（即若$N<M\lhd G$，则$M=G$）。

引理3.4.2 （1）有限群必有组成列；

（2）可解列的加细仍为可解列；

（3）一个正规列是组成列的充要条件是它没有真加细。

证明 （1）设 G_1 为G的极大正规子群，则G/G_1为单群。再令 G_2 为 G_1 的极大正规子群，…。由于$|G|>|G_1|>|G_2|>\cdots$，从而有 n 使 $G_n=\{1\}$。于是$G>G_1>\cdots>G_n=\{1\}$就是G的一

个组成列。

（2）和（3）的证明留给读者进行。

定理3.4.5 群G可解$\Longleftrightarrow G$有可解列。

证明 若G可解，则$G\geqslant G^{(1)}\geqslant\cdots\geqslant G^{(n)}=\{1\}$就是$G$的一个可解列。反之，若$G=G_0\geqslant G_1\geqslant\cdots\geqslant G_n=\{1\}$是可解列，则$G/G_1$为阿贝尔群，于是$G_1\geqslant G^{(1)}$。同样，由$G_1/G_2$为阿贝尔群，于是$G_2\geqslant G_1^{(1)}\geqslant G^{(2)}$，因此归纳可得$G_i\geqslant G^{(i)}$（对每个$i$），所以$\{1\}=G_n\geqslant G^{(n)}$，即$G^{(n)}=\{1\}$，从而$G$可解。

例3.4.4 $D_n>\langle a\rangle>\{1\}$是可解列，其中$a$是$D_n$中任意$n$阶元素，因此$D_n(n\geqslant 3)$为可解群。

例3.4.5 设$|G|=pq$，其中p和q为素数，$p>q$。这时，G中有p阶元素a，且$\langle a\rangle$为G的正规子群（西洛定理）。于是$G>\langle a\rangle>\{1\}$为可解列，即G为可解群。

练习3.4.8 有限群G是可解群$\Longleftrightarrow G$有组成列，其非平凡因子均是素阶循环群。

练习3.4.9 求D_4和$S_3\times Z_2$的全部组成列。求S_4和D_6的组成列因子。

练习3.4.10 群的组成列是具有极大长度的正规列。

练习3.4.11 设$H\leqslant C(G)$，且G/H为幂零群，则G是幂零群。

练习3.4.12 设p，q，r为三个素数，则pqr阶群必为可解群。

一个群可以有许多组成列，下面要证明组成列的非平凡因子集合不依赖于组成列的选择，即是G本身的不变量。

定义3.4.6 群G的两个正规列S和T叫作**等价的**，是指在S和T的非平凡因子之间存在一一对应，并且对应的因子是同构的。

由定义可知，群G的两个等价正规列不一定有同样多项，但有相同的长度（即同样多个非平凡因子）。此外，正规列的等价显然是等价关系。

引理 3.4.3 若 S 是群 G 的一个组成列，则 S 的每个加细均与 S 等价。

证明 设 S 为 $G=G_0\geqslant G_1\geqslant\cdots\geqslant G_n=\{1\}$。由引理 3.4.2 知 S 没有真的加细，从而 S 的加细只是再加入某些 G_i，即只能多出一些平凡因子，从而与 S 等价。

引理3.4.4（扎森浩斯(Zassenhaus)） 设 $A'\lhd A$，$B'\lhd B$，则 $A'(A\cap B')\lhd A'(A\cap B)$，$B'(A'\cap B)\lhd B'(A\cap B)$，并且 $A'(A\cap B)/A'(A\cap B')\cong B'(A\cap B)/B'(A'\cap B)$。

证明 由 $B'<B$ 可知，$A\cap B'=(A\cap B)\cap B'\lhd(A\cap B)$，同样有 $A'\cap B\lhd A\cap B$，因此，$D=(A'\cap B)(A\cap B')\lhd A\cap B$，$A'(A\cap B)\leqslant A$。现在定义

$$f: A'(A\cap B)\to(A\cap B)/D,$$

办法是：对于 $a\in A'$，$C\in A\cap B$，令 $f(ac)=Dc$。这是可定义的，因为，当 $ac=a'c'$，$a'\in A'$，$c'\in A\cap B$，则 $c'c^{-1}=(a')^{-1}a\in(A\cap B)\cap A'=A'\cap B\leqslant D$，从而 $Dc=Dc'$。进而，对于 a_1，$a_2\in A'$，c_1，$c_2\in A\cap B$。由于 $A'\lhd A$，可知 $c_1a_2=a_3c_1$，$a_3\in A'$，$f((a_1c_1)(a_2c_2))=f(a_1a_3c_1c_2)=Dc_1c_2=Dc_1\cdot Dc_2=f(a_1c_1)f(a_2c_2)$。从而 f 为同态，显然 f 是满同态。最后，$aca\in\mathrm{Ker}f\Longleftrightarrow c\in D\Longleftrightarrow c=a_1c_1$，$a_1\in A'\cap B$，$c_1\in A\cap B'\Longleftrightarrow$

$$ac=(aa_1)c_1\in A'(A\cap B'),$$

$\mathrm{Ker}f=A'(A\cap B')$，于是 $A'(A\cap B')\lhd A'(A\cap B)$，并且 $A'(A\cap B)/A'(A\cap B')\cong(A\cap B)/D$。同样，可证 $B'(A'\cap B)\lhd B(A\cap B)$，并且 $B'(A\cap B)/B'(A'\cap B)\cong(A\cap B)/D$。由此即得引理。

定理 3.4.6（施赖埃尔(Schreier)） 群 G 的任意两个正规列均有等价的正规加细列。

证明 设 $G=G_0\geqslant G_1\geqslant\cdots\geqslant G_n$ 和 $G=H_0\geqslant H_1\geqslant\cdots\geqslant H_m$ 是两个正规列。令 $G_{n+1}=\{1\}=H_{m+1}$。对于 $0\leqslant i\leqslant n$，则有

$$G_i=G_{i+1}(G_i\cap H_0)\geqslant G_{i+1}(G_i\cap H_1)\geqslant\cdots\geqslant G_{i+1}(G_i\cap H_{m+1})=G_{i+1}。$$

对每个 $0\leqslant j\leqslant m$，由引理 3.4.5 知 $G_{i+1}(G_i\cap H_{j+1})\lhd G_{i+1}$

$\times(G_i \cap H_j)$。在 G_i 和 G_{i+1} 之中插入上述诸群，如果以 $G(i, j)$ 表示 $G_{i+1}(G_i \cap G_j)$，则给出 $G_0 \geqslant G_1 \geqslant \cdots \geqslant G_n$ 的正规加细列：

$$
\begin{aligned}
G = G(0,\ 0) &\geqslant G(0,\ 1) \geqslant \cdots \geqslant G(0,\ m) \\
&\geqslant G(1,\ 0) \geqslant G(1,\ 1) \geqslant \cdots \geqslant G(1,\ m) \\
&\geqslant G(2,\ 0) \geqslant \cdots \geqslant G(n-1,\ m) \geqslant G(n,\ 0) \\
&\geqslant G(n,\ 1) \geqslant \cdots \geqslant G(n,\ m),
\end{aligned}
$$

其中 $G(i,\ 0) = G_i$。这个加细列共 $(n+1)(m+1)$ 项。同样若令 $H(i,\ j) = H_{j+1}(G_i \cap H_j)$，则 $H(0,\ j) = H_j$，从而有 $G = H_0 \geqslant H_1 \geqslant \cdots \geqslant H_m$ 的加细：

$$
\begin{aligned}
G = H(0,\ 0) &\geqslant H(1,\ 0) \geqslant \cdots \geqslant H(n,\ 0) \geqslant H(0,\ 1) \\
&\geqslant H(1,\ 1) \geqslant \cdots \geqslant H(n,\ 1) \geqslant H(0,\ 2) \geqslant \cdots \\
&\geqslant H(n,\ m-1) \geqslant H(0,\ m) \geqslant H(1,\ m) \geqslant \cdots \\
&\geqslant H(n,\ m)。
\end{aligned}
$$

这个加细列也有 $(n+1)(m+1)$ 项。由引理 3.4.4 知道

$$
\frac{G(i,\ j)}{G(i,\ j+1)} = \frac{G_{i+1}(G_i \cap H_j)}{G_{i+1}(G_i \cap H_{j+1})}
\cong \frac{H_{j+1}(G_i \cap H_j)}{H_{j+1}(G_{i+1} \cap H_j)} = \frac{H(i,\ j)}{H(i+1,\ j)}
$$

$(0 \leqslant i \leqslant n,\ 0 \leqslant j \leqslant m)$。从而两个加细列是等价的。

定理3.4.7（约当-赫尔德(Jordan-Hölder)） 群 G 的任意两个组成列均等价。因此，若群 G 有组成列，则其非平凡因子集合（这是一些单群）为 G 的不变量（即与组成列的选取无关）。特别地，群 G 的任意两个组成列有相同的长度。

证明 由于组成列都是正规列，从而 G 的任意两个组成列均有等价的加细。但是组成列的加细等价于自身，从而 G 的任意两个组成列均等价。

例 3.4.6 对于群 A_4，它有如下两个组成列：

$$A_4 \rhd \langle(1234)\rangle \rhd \langle(12)(34)\rangle \rhd 1,$$

$$A_4 \rhd M \rhd \langle(12)(34)\rangle \rhd 1。$$

其中 $M = \{1,\ (12)(34),\ (13)(24),\ (14)(23)\}$，对应的非平凡因子为 $\{Z_3,\ Z_2,\ Z_2\}$。

第四章　有 限 点 群

在自然科学中，对称的观念是最基本的观念之一。实数域上三维欧几里得空间中一个物体的对称性可以用它的对称群描述，即可以用使物体在空间中不动的变换构成的群来描述（这里把物体作为刚体考虑）。在物理学、化学和其它自然科学中，特别重要的对称群是有限点群，它可用于描述物理结构及分子的对称性等。

这章的主要目的有二个，一是讨论有限点群的分类，二是给出有限点群的具体表示，即把它们作为某个几何图形对称群的子群。最后得到32个晶体点群，它们恰好对应着结晶学中的32个晶类。

§4.1　三维空间中的正交群

设$\mathbb{R}$是实数域，$\mathbb{R}^3$是域$\mathbb{R}$上的三维向量空间，$\{\boldsymbol{e}_1, \boldsymbol{e}_2, \boldsymbol{e}_3\}$是$\mathbb{R}^3$的一组基底。对于$\mathbb{R}^3$中的任何二个向量$\boldsymbol{x}$和$\boldsymbol{y}$，其中

$$\boldsymbol{x}=x_1\boldsymbol{e}_1+x_2\boldsymbol{e}_2+x_3\boldsymbol{e}_3,$$

$$\boldsymbol{y}=y_1\boldsymbol{e}_1+y_2\boldsymbol{e}_2+y_3\boldsymbol{e}_3,$$

有双线性型（或双线性函数）

$$\langle\boldsymbol{x},\ \boldsymbol{y}\rangle=x_1y_1+x_2y_2+x_3y_3。$$

这个双线性型定义了向量空间$\mathbb{R}^3$的内积，从而使$\mathbb{R}^3$成为欧几里得空间。这是一个度量空间。向量$\boldsymbol{x}$的模$\|\boldsymbol{x}\|=\langle\boldsymbol{x},\ \boldsymbol{x}\rangle^{1/2}$定义为向量的长度，而向量$\boldsymbol{x}$和$\boldsymbol{y}$之间的夹角$\varphi$的余弦是$\cos\varphi=\dfrac{\langle\boldsymbol{x},\ \boldsymbol{y}\rangle}{\|\boldsymbol{x}\|\cdot\|\boldsymbol{y}\|}$。如果$\cos\varphi=0$，则说向量$\boldsymbol{x}$和向量$\boldsymbol{y}$是正交的。

我们说作用在$\mathbb{R}^3$上的线性变换O是保长的，如果对所有$\mathbb{R}^3$中的向量$\boldsymbol{x}$，O满足$\langle O\boldsymbol{x},\ O\boldsymbol{x}\rangle=\langle\boldsymbol{x},\ \boldsymbol{x}\rangle$。由此容易推出，线性

变换是保长的当且仅当保持任何二个向量的内积不变，即$\langle Ox, Oy\rangle=\langle x, y\rangle$。进而，如果$Ox=0$，必定有$x=0$。利用此性质不难看出，$\mathbb{R}^3$上的保长线性变换把线性无关向量仍变成线性无关向量，从而得出保长线性变换必是可逆线性变换。

命题 4.1.1 三维欧几里得空间$\mathbb{R}^3$中的保长线性变换全体成群，称为3维空间$\mathbb{R}^3$的**实正交群**，用$O_3(\mathbb{R})$表示，或简单地记为$O(3)$。$O(3)$的元（或元素）称为正交变换。

由于$O(3)$的元素保持内积不变，故保持正交关系不变，由此而得正交变换之名。

取$\mathbb{R}^3$的一组标准正交基$\{e_1, e_2, e_3\}$，即这是$\mathbb{R}^3$的一组基底，而且满足

$$\langle e_i, e_j\rangle=\delta_{ij},$$

其中

$$\delta_{ij}=\begin{cases}0, & 当\ i\neq j\\ 1, & 当\ i=j。\end{cases}$$

设正交变换$\mathscr{T}$在这个基底下的矩阵表示为T，$T=(t_{ij})$，即$\mathscr{T}e_i=\sum_{j=1}^{3}t_{ji}e_j$。由于$\langle\mathscr{T}e_i, \mathscr{T}e_j\rangle=\langle e_i, e_j\rangle=\delta_{ij}$，和

$$\langle\mathscr{T}e_i, \mathscr{T}e_j\rangle=\left\langle\sum_{k=1}^{3}t_{ki}e_k, \sum_{l=1}^{3}t_{lj}e_l\right\rangle=\sum_{l=1}^{3}t_{lj}t_{li}。$$

有

$$T\cdot T'=E, \tag{4-1}$$

其中T'表示矩阵T的转置阵，E是单位阵。实际上，具有性质(4-1)的矩阵就是熟知的三维空间的实正交阵。实正交矩阵全体成群，仍将这个群记为$O(3)$，在映射$\mathscr{T}\to T$之下，它同构于正交变换全体所成的群。显然，正交矩阵T所决定的线性变换$\mathscr{T}$必定是保长的。以后，为方便起见，有时采用变换进行讨论，有时则用矩阵进行讨论。

引理 4.1.1 如果$T\in O(3)$，则$\det T=\pm 1$。

证明 因为$T\cdot T'=E$，所以$(\det T)^2=1$，即$\det T=\pm 1$。显然，E和$I=-E$都是$O(3)$的元素。$\det E=1$，$\det I=-1$。令$\mathscr{I}$是矩阵I决定的线性变换，对所有$x\in\mathbb{R}^3$，$\mathscr{I}x=-x$。通常称$\mathscr{I}$为**反演变换**或**反演**，$\mathscr{I}^2=E$。

二个元素的集合$\{1,-1\}$，按平常的数乘运算形成一个2阶循环群C_2。考虑$O(3)$到C_2的映射$\det.:O(3)\to C_2$，它将$T\in O(3)$映到它的行列式$\det T$，易见，映射$\det.$是一个群同态。用$SO(3)$表示$\det.$的核，则有

$$SO(3)=\{T\in O(3)|\det T=1\},$$

$SO(3)\lhd O(3)$和$O(3)/SO(3)\cong C_2$。有时将$SO(3)$也记为$O(3)^+$。通常称$SO(3)$为特殊正交群，$SO(3)$的元素称为正常转动或转动。$O(3)$相对正规子群$SO(3)$分解为2个陪集，取E和I分别为陪集代表元。于是$O(3)=SO(3)\cup I\cdot SO(3)$（这里是集合的并）。易知，行列式为$-1$的正交阵$T'$可表成为$T'=I\cdot T$，其中$T\in SO(3)$，即$T'\in I\cdot SO(3)$，称$T'$为**转动反演**或**非正常转动**。

下面将证明：$SO(3)$的元素是由$\mathbb{R}^3$中绕过原点的轴的所有转动组成（这是称$SO(3)$的元素为转动的原因），而$O(3)$是由这些转动和转动反演组成。

定理 4.1.1 设$\mathscr{A}\in SO(3)$，则存在一个单位向量$\boldsymbol{f}_3\in\mathbb{R}^3$，$\|\boldsymbol{f}_3\|=1$，使得$\mathscr{A}\boldsymbol{f}_3=\boldsymbol{f}_3$。如果$\mathscr{A}\neq\mathscr{E}$，这里$\mathscr{E}$是单位变换，那么由$\pm\boldsymbol{f}_3$表示的直线，即过$\boldsymbol{f}_3$的直线，称为变换$\mathscr{A}$的转动轴。

证明 如果$\boldsymbol{f}_3$满足$\mathscr{A}\boldsymbol{f}_3=\boldsymbol{f}_3$，$\|\boldsymbol{f}_3\|=1$，这说明$\boldsymbol{f}_3$是$\mathscr{A}$的特征根为1的单位特征向量。因此，要证明这样的$\boldsymbol{f}_3$存在，只需证明$\lambda=1$是$\mathscr{A}$的一个特征根即可。设$A$是$\mathscr{A}$的矩阵表示，这等价于证明$\det(A-E)=0$。由于$\det(A-E)=\det(A-E)'$和$\det A=1$，$A'=A^{-1}$，有

$$\begin{aligned}\det(A-E)&=\det(A'-E)=\det(A^{-1}-E)\\&=\det A^{-1}(E-A)=\det(E-A)\\&=(-1)^3\det(A-E)=-\det(A-E),\end{aligned}$$

于是 $\det(A-E)=0$，$\lambda=1$ 是$\mathscr{A}$的一个特征根。定理得证。

选取向量 f_1 和 f_2，使得$\{f_1, f_2, f_3\}$成为 $\mathbb{R}^3$ 的一组标准正交基，即$\langle f_i, f_j\rangle=\delta_{ij}$。找出交换$\mathscr{A}$相对这个基底的矩阵表示。为此，只要计算$\mathscr{A}f_i$，$i=1, 2, 3$。假设

$$\mathscr{A}f_1=\alpha_1 f_1+\alpha_2 f_2+\alpha_3 f_3,$$
$$\mathscr{A}f_2=\beta_1 f_1+\beta_2 f_2+\beta_3 f_3,$$
$$\mathscr{A}f_3=f_3。$$

由于$\langle\mathscr{A}f_i, \mathscr{A}f_j\rangle=\langle f_i, f_j\rangle=\delta_{ij}$，$1\leqslant i, j\leqslant 3$，得到 $\alpha_3=\beta_3=0$，$\alpha_1\beta_1+\alpha_2\beta_2=0$，$\alpha_1^2+\alpha_2^2=\beta_1^2+\beta_2^2=1$。那么$\mathscr{A}$在基底$\{f_1, f_2, f_3\}$之下的矩阵可表示为

$$A=\begin{pmatrix}\alpha_1 & \beta_1 & 0\\ \alpha_2 & \beta_2 & 0\\ 0 & 0 & 1\end{pmatrix},$$

A具有性质

$$\begin{cases}\alpha_1^2+\alpha_2^2=1 & (4\text{-}2)\\ \beta_1^2+\beta_2^2=1 & (4\text{-}3)\\ \alpha_1\beta_1+\alpha_2\beta_2=0 & (4\text{-}4)\\ \alpha_1\beta_2-\alpha_2\beta_1=1 & (4\text{-}5)\end{cases}$$

式（4-2）和（4-3）表示向量$\mathscr{A}f_1=(\alpha_1, \alpha_2, 0)$和$\mathscr{A}f_2=(\beta_1, \beta_2, 0)$是单位向量，式（4-4）表示它们是正交的，式(4-5)表示向量（α_1，α_2，0）按反时针方向旋转$\frac{\pi}{2}$后，成为向量$(\beta_1, \beta_2, 0)$，如图 4-1 所示。于是得到满足式（4-2）到式（4-5）的唯一解：

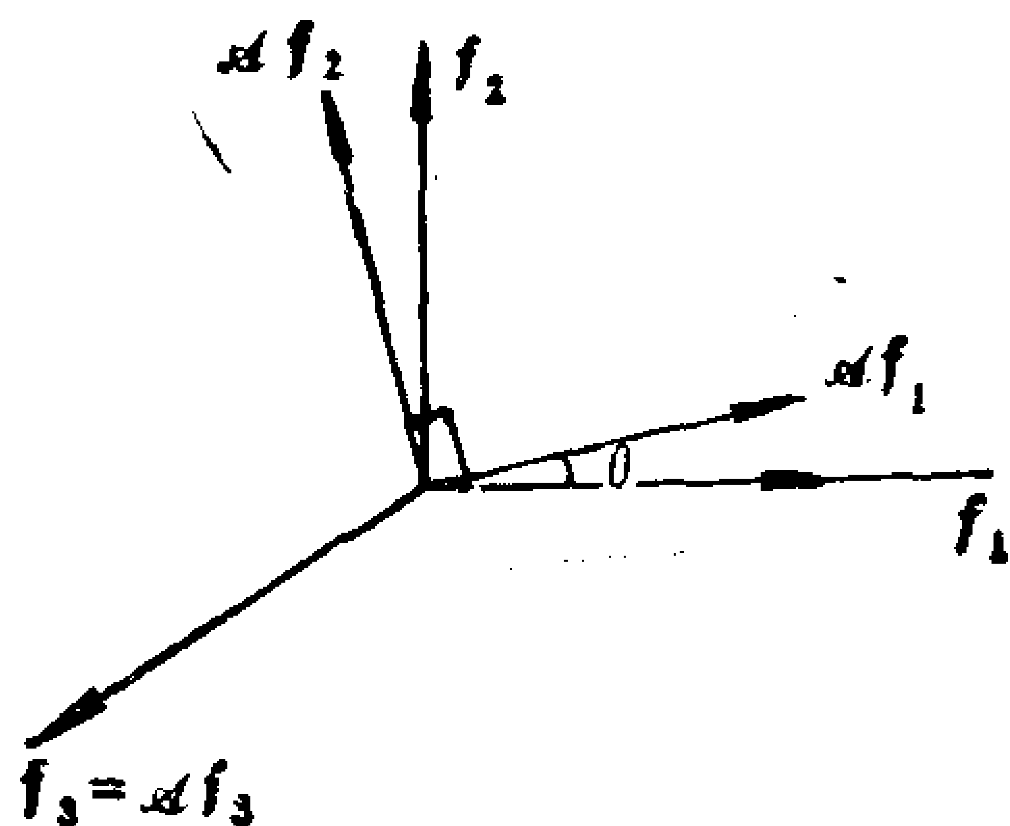


图 4-1

$$\alpha_1=\beta_2=\cos\theta,\quad \alpha_2=-\beta_1=\sin\theta,\quad 0\leqslant\theta<2\pi。$$

因此

$$A=\begin{pmatrix}\cos\theta & -\sin\theta & 0\\ \sin\theta & \cos\theta & 0\\ 0 & 0 & 1\end{pmatrix}\qquad 0\leqslant\theta<2\pi,$$

其中 θ 是向量 $\boldsymbol{f}_1$ 和$\mathscr{A}\boldsymbol{f}_1$之间的夹角。对于 $\mathbb{R}^3$ 中任意向量 $\boldsymbol{x}=a_1\boldsymbol{f}_1+a_2\boldsymbol{f}_2+a_3\boldsymbol{f}_3$，其坐标表示是 $\boldsymbol{x}=(a_1,\ a_2,\ a_3)$，经过变换$\mathscr{A}$作用后变为

$$\mathscr{A}\boldsymbol{x}=A\begin{pmatrix}a_1\\ a_2\\ a_3\end{pmatrix}=(a_1\cos\theta-a_2\sin\theta,\ \ a_1\sin\theta+a_2\cos\theta,\ a_3)。$$

根据熟知的解析几何知识，这个结果表明变换$\mathscr{A}$的作用是绕$\boldsymbol{f}_3$轴反时针旋转 θ 角。通常采用符号$\mathscr{A}=C_k(\theta)$ 表示绕过原点的固定轴的转动变换或转动，其中 $\boldsymbol{k}$ 表示转动轴，θ 表示转角。转动方向由右手法则而定。由几何直观得结果

$$C_k(\theta+\varphi)=C_k(\theta)\cdot C_k(\varphi)=C_k(\varphi)\cdot C_k(\theta),$$

$$C_k(\theta)=C_{-k}(2\pi-\theta)=C_{-k}(-\theta)。$$

从变换角度看，$C_k(\alpha)=C_k(\alpha+2\pi)$。于是，得到系 4.1.1。

系4.1.1 特殊正交群 $SO(3)$ 是由 $\mathbb{R}^3$ 中绕过原点的轴的所有转动组成。

关于转动反演也有简单的几何解释。设$\mathscr{A}'$是任意给定的一个转动反演。那么$\mathscr{A}'=I\mathscr{A}$，其中$\mathscr{A}\in SO(3)$。由系 4.1.1，有 $\boldsymbol{k}$ 和 θ，使得

$$\mathscr{A}'=I\mathscr{A}=IC_k(\pi+\theta)=IC_k(\pi)\cdot C_k(\theta)。$$

令 $\sigma_k=IC_k(\pi)$，从几何直观看，σ_k 是对经过 $\mathbb{R}^3$ 的原点并垂直于 $\boldsymbol{k}$ 的平面的反射。σ_k 在标准正交基底 $\{\boldsymbol{f}_1,\ \boldsymbol{f}_2,\ \boldsymbol{f}_3=\boldsymbol{k}\}$下的矩阵表示是

$$\sigma_k=\begin{pmatrix}-1 & 0 & 0\\ 0 & -1 & 0\\ 0 & 0 & -1\end{pmatrix}\begin{pmatrix}-1 & 0 & 0\\ 0 & -1 & 0\\ 0 & 0 & 1\end{pmatrix}$$

$$=\begin{pmatrix}1 & 0 & 0\\ 0 & 1 & 0\\ 0 & 0 & -1\end{pmatrix},$$

如图 4-2 所示。

因此，任何一个转动反演都是先施行对于某个轴 $\boldsymbol{k}$ 的转动变换，再接着作对于垂直于$\boldsymbol{k}$的平面的反射变换的结果。通常用$S_k(\theta)=\sigma_k\cdot C_k(\theta)$ 表示转动反演。

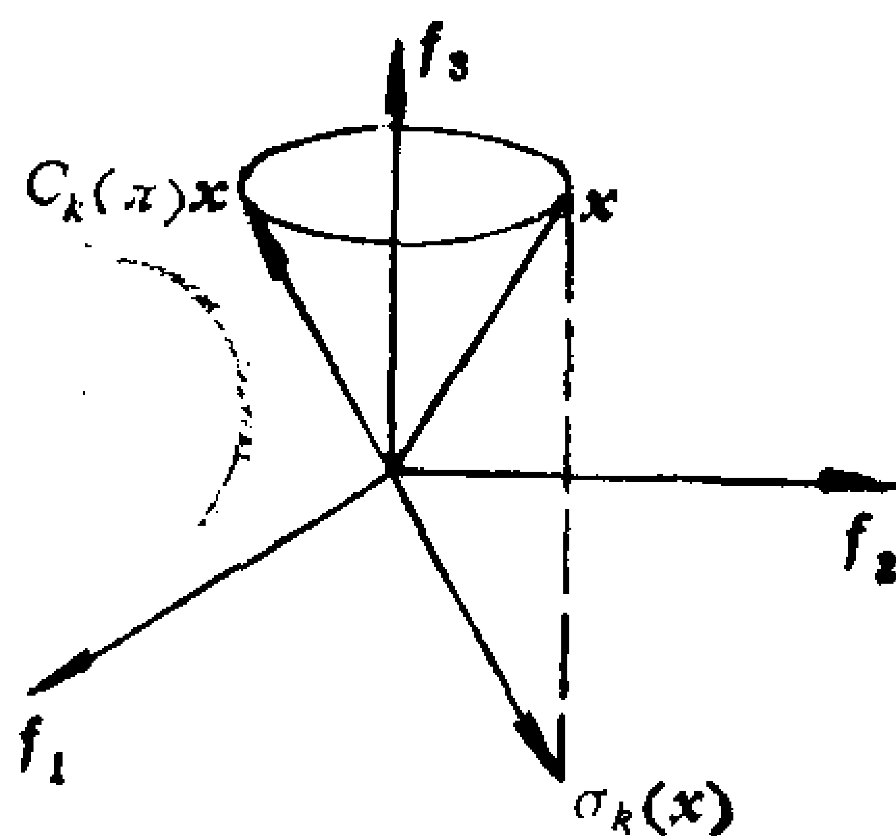


图 4-2

系4.1.2 实正交群$O(3)$是由绕过原点的轴的转动和转动反演组成。

下边讨论群$SO(3)$和$O(3)$的共轭类。

从线性代数知道，若$\mathbb{R}^3$的一个线性变换$\mathscr{A}$在基底$\{\boldsymbol{e}_1, \boldsymbol{e}_2, \boldsymbol{e}_3\}$之下的矩阵表示是$A$，那么线性变换$\mathscr{P}\mathscr{A}\mathscr{P}^{-1}$在基底$\{\mathscr{P}\boldsymbol{e}_1, \mathscr{P}\boldsymbol{e}_2, \mathscr{P}\boldsymbol{e}_3\}$之下的矩阵表示仍然是$A$。由此，若转动$C_k(\theta)$在基底$\{\boldsymbol{f}_1, \boldsymbol{f}_2, \boldsymbol{f}_3=\boldsymbol{k}\}$之下的矩阵表示是

$$\begin{pmatrix} \cos\theta & -\sin\theta & 0 \\ \sin\theta & \cos\theta & 0 \\ 0 & 0 & 1 \end{pmatrix} \tag{4-6}$$

那么$C_k(\theta)$的共轭元$\mathscr{A}C_k(\theta)\mathscr{A}^{-1}$(其中$\mathscr{A}\in SO(3)$)在基底$\{\mathscr{A}\boldsymbol{f}_1, \mathscr{A}\boldsymbol{f}_2, \mathscr{A}\boldsymbol{f}_3=\mathscr{A}\boldsymbol{k}\}$之下的矩阵表示仍然是式(4-6)，于是有

$$\mathscr{A}C_k(\theta)\mathscr{A}^{-1}=C_{\mathscr{A}k}(\theta)。$$

另一方面，$C_h(\theta)$与$C_k(\theta)$在$SO(3)$中共轭，其中$\boldsymbol{h}$是任意给定的一个向量。实际上，$C_k(\theta)$在一组标准正交基$\{\boldsymbol{f}_1, \boldsymbol{f}_2, \boldsymbol{f}_3\}$之下有如式(4-6)的矩阵表示，而$C_h(\theta)$在另一组标准正交基$\{\boldsymbol{h}_1, \boldsymbol{h}_2, \boldsymbol{h}_3\}$之下也有同样的如式(4-6)的矩阵表示。令线性变换$\mathscr{A}$将$\boldsymbol{f}_i$变到$\boldsymbol{h}_i(i=1, 2, 3)$，即$\mathscr{A}\boldsymbol{f}_i=\boldsymbol{h}_i$，那么$\mathscr{A}\in O(3)$。于是有

$$\mathscr{A}C_k(\theta)\mathscr{A}^{-1}=C_{\mathscr{A}k}(\theta)=C_h(\theta)。$$

这里需注意，$C_h(\theta)=C_{\alpha h}(\theta)$，其中$\alpha$是正实数。如果$\mathscr{A}\in SO(3)$，那么$C_k(\theta)$与$C_h(\theta)$在$SO(3)$中共轭；如果$\mathscr{A}\in$

$O(3)\backslash SO(3)$，则有$\mathscr{I}\mathscr{A}\in SO(3)$和

$$(\mathscr{I}\mathscr{A})C_k(\theta)(\mathscr{I}\mathscr{A})^{-1}=C_{-h}(\theta)。$$

设变换$\mathscr{B}$在基底$\{\boldsymbol{h}_1, \boldsymbol{h}_2, \boldsymbol{h}_3\}$的矩阵表示为

$$\begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix},$$

那么$\mathscr{B}\in SO(3)$，$\mathscr{B}C_{-h}(\theta)\mathscr{B}^{-1}=C_{-\mathscr{B}(h)}$[●]$(\theta)=C_h(\theta)$。再考虑$C_h(\pi+\theta)$，其中$0<\theta<\pi$。有

$C_h(\pi+\theta)=C_h(\pi+\theta-2\pi)=C_{-h}(\pi-\theta)=C_{-h}(\theta')$，其中$0<\theta'=\pi-\theta<\pi$。最后，若$C_k(\theta_1)=C_h(\theta_2)$，其中$0\leqslant\theta_1, \theta_2\leqslant\pi$，必定有$\boldsymbol{k}=\pm\alpha\boldsymbol{h}$ ($\alpha>0$)。不失一般性，设$\alpha=1$。对于$C_h(\theta_1)=C_k(\theta_2)$，当且仅当$\theta_1=\theta_2$；对于$C_k(\theta_1)=C_{-k}(\theta_2)$，当且仅当$\theta_1=\theta_2=\pi$。综上所述，得到如下命题。

命题4.1.2 $SO(3)$的任何一个共轭类都由转角相同的所有转动组成。若转角为θ的共轭类由$C(\theta)$表示，那么$SO(3)$的全体共轭类为集合

$$\{C(\theta)\mid 0\leqslant\theta\leqslant\pi\}。$$

进而讨论$O(3)$的共轭类。先考虑

$$\sigma_k C_h(\theta)\sigma_k^{-1}=IC_k(\pi)C_h(\theta)C_k(\pi)^{-1}I^{-1}$$
$$=C_{C_k(\pi)h}(\theta)=C_{-\sigma_k(h)}(\theta)。$$

由此，对于任意的$\mathscr{A}\in O(3)$，有

$$\mathscr{A}C_h(\theta)\mathscr{A}^{-1}=C_{\varepsilon\mathscr{A}h}(\theta),$$

其中$\varepsilon=\det\mathscr{A}$。对于任意的$\mathscr{A}\in O(3)$，再考虑

$$\mathscr{A}S_h(\theta)\mathscr{A}^{-1}=\mathscr{A}\sigma_h C_h(\theta)\mathscr{A}^{-1}$$
$$=\mathscr{A}\mathscr{I}C_h(\pi)C_h(\theta)\mathscr{A}^{-1}=\mathscr{I}C_{\varepsilon\mathscr{A}h}(\pi)C_{\varepsilon\mathscr{A}h}(\theta)$$
$$=\sigma_{\varepsilon\mathscr{A}h}C_{\varepsilon\mathscr{A}h}(\theta)=S_{\varepsilon\mathscr{A}h}(\theta)。$$

由此结果，再仿照前面的讨论，便得到如下命题。

命题4.1.3 $O(3)$的共轭类有二种类型：一种是由所有转

● $\mathscr{B}(\boldsymbol{h})=\mathscr{B}\boldsymbol{h}$

角为 θ（$0\leqslant\theta\leqslant\pi$）的转动组成的共轭类。另一种是由所有转角为 θ'（$0\leqslant\theta'\leqslant\pi$）的转动反演组成的共轭类。

§4.2 欧几里得群

欧几里得群与大家熟知的欧几里得几何有着密切的关系。三维空间的正交群和物理学中的刚体运动群都是本节介绍的欧几里得群的子群。

定义 4.2.1 三维欧几里得空间 $\mathbb{R}^3$ 到 $\mathbb{R}^3$ 之上的保持任意两点之间距离不变的变换 T，即

$$\|T\boldsymbol{x}-T\boldsymbol{y}\|=\|\boldsymbol{x}-\boldsymbol{y}\|,\quad x, y\in\mathbb{R}^3,$$

称为**等距变换**。

注意；这里不要求变换 T 是线性的，而只是把 T 看作保持距离不变的 $\mathbb{R}^3$ 中元素的一个置换。显然，等距变换必定是保长变换。令 $E(3)$ 是作用在 $\mathbb{R}^3$ 上的所有等距变换的集合，有以下定理。

定理 4.2.1 $E(3)$ 成群。称 $E(3)$ 为三维空间 $\mathbb{R}^3$ 的**欧几里得群**。

证明 显然，恒等变换是在 $E(3)$ 中。对于 $T\in E(3)$，由于 T 是 $\mathbb{R}^3$ 到 $\mathbb{R}^3$ 之上的等距变换，则它是 $\mathbb{R}^3$ 到 $\mathbb{R}^3$ 之上的一一变换，因此 T 是 $\mathbb{R}^3$ 上的可逆变换。能验证 T^{-1} 也是等距变换。设 $\boldsymbol{x}$ 和 $\boldsymbol{y}$ 是 $\mathbb{R}^3$ 中任意两点，而且 $T^{-1}\boldsymbol{x}=\boldsymbol{u}$，$T^{-1}\boldsymbol{y}=\boldsymbol{v}$。$\|T^{-1}\boldsymbol{x}-T^{-1}\boldsymbol{y}\|=\|\boldsymbol{u}-\boldsymbol{v}\|=\|T\boldsymbol{u}-T\boldsymbol{v}\|=\|\boldsymbol{x}-\boldsymbol{y}\|$，于是 $T^{-1}\in E(3)$。若 T_1，$T_2\in E(3)$，易验 $T_1\cdot T_2\in E(3)$。因此 $E(3)$ 成群。

系 4.2.1 $O(3)$ 是 $E(3)$ 的子群，而且 $O(3)$ 的每个元素均使原点保持不动。

进而，有如下定理。

定理 4.2.2 使原点不变的 $\mathbb{R}^3$ 的等距变换一定是线性变换。因此，$O(3)$ 是由 $E(3)$ 中使原点不变的等距变换全体所组成。

为了证明此定理，需要几个引理。

在欧几里得空间中，如果两个点是不同的，则说两个点是无

关的；如果三个点不共线，则说这三个点是无关的；如果四个点不共面，则说这四个点是无关的。

引理 4.2.1 设 T 为等距变换，若 T 有两个无关的固定点，则过这两点的直线上的每点都是 T 的固定点；若 T 有三个无关的固定点，则过这三点的平面上的每点都是 T 的固定点；若 T 有四个无关的固定点，则 T 是恒等变换。

证明 设 $\boldsymbol{x}$ 和 $\boldsymbol{y}$ 是 T 的两个无关固定点，$\boldsymbol{w}$ 是过 $\boldsymbol{x}$ 和 $\boldsymbol{y}$ 的直线上 l 任意选定的一点。由 $\boldsymbol{w}$ 相对 $\boldsymbol{x}$ 和 $\boldsymbol{y}$ 的位置，有 $\|\boldsymbol{w}-\boldsymbol{x}\|+\|\boldsymbol{w}-\boldsymbol{y}\|=\|\boldsymbol{x}-\boldsymbol{y}\|$，或者 $\|\boldsymbol{w}-\boldsymbol{y}\|-\|\boldsymbol{w}-\boldsymbol{x}\|=\|\boldsymbol{x}-\boldsymbol{y}\|$，或者 $\|\boldsymbol{w}-\boldsymbol{x}\|-\|\boldsymbol{w}-\boldsymbol{y}\|=\|\boldsymbol{x}-\boldsymbol{y}\|$。根据初等几何中三角形两边长度之和与第三边长度的关系，上边的任何一种情况都有 $T\boldsymbol{w}$ 在过 $\boldsymbol{x}$ 和 $\boldsymbol{y}$ 的直线上。进而，$T\boldsymbol{w}$ 在以 $\boldsymbol{x}$ 为中心，以 $\|\boldsymbol{x}-\boldsymbol{w}\|$ 长为半径的球面上，同时在以 $\boldsymbol{y}$ 为中心，以 $\|\boldsymbol{y}-\boldsymbol{w}\|$ 长为半径的球面上。因此，$T\boldsymbol{w}=\boldsymbol{w}$，$T$ 使直线 l 上每点不动。

设 $\boldsymbol{x}$，$\boldsymbol{y}$ 和 $\boldsymbol{z}$ 是 T 的三个无关固定点。过 $\boldsymbol{x}$、$\boldsymbol{y}$ 的直线为 l_1，过 $\boldsymbol{y}$、$\boldsymbol{z}$ 的直线为 l_2 和过 $\boldsymbol{x}$、$\boldsymbol{z}$ 的直线为 l_3。由上面的讨论，T 使这三条直线 l_1、l_2 和 l_3 上的每点都保持不动。在过 $\boldsymbol{x}$，$\boldsymbol{y}$ 和 $\boldsymbol{z}$ 这三点的平面上任取一点 $\boldsymbol{w}$。设 $\boldsymbol{w}$ 不在 l_1，l_2 和 l_3 上，过 $\boldsymbol{x}$ 和 $\boldsymbol{w}$ 的直线 l 必定与过 $\boldsymbol{y}$ 和 $\boldsymbol{z}$ 的直线 l_2 相交。根据上面的讨论，T 使 $\boldsymbol{x}$ 和交点不动，因而 T 使 $\boldsymbol{w}$ 不动。若 $\boldsymbol{w}$ 在某个直线 l_i 上，显然 T 使 $\boldsymbol{w}$ 不动。

由完全类似的讨论可知，若 T 使四个无关点不动，则 T 使空间中每个点都不动；即 T 是恒等变换。

引理 4.2.2 如果等矩变换 T 有至少 k 个无关固定点，k 为 0，1，2，3，4 之一，则 T 可分解为至多 $4-k$ 个反射之积。

证明 首先假设 $k=4$。由引理 4.2.1，这时等矩变换为恒等变换，它是零个反射之积。如果 $T\neq E$，必定有 $k\leqslant 3$ 和存在一点 $\boldsymbol{y}$，使得 $T\boldsymbol{y}\neq\boldsymbol{y}$。设 T 的 k 个无关固定点是 $\boldsymbol{x}_1,\cdots,\boldsymbol{x}_k$，过线段〔$\boldsymbol{y}$，$T\boldsymbol{y}$〕中点、且垂直于过 $\boldsymbol{y}$ 和 $T\boldsymbol{y}$ 的直线 l 的平面为 A。由于 $T\boldsymbol{x}_i=\boldsymbol{x}_i$ 和 $\|\boldsymbol{x}_i-\boldsymbol{y}\|=\|\boldsymbol{x}_i-T\boldsymbol{y}\|$，则 $\boldsymbol{x}_i$ 全都位于平面 A 上，于

是等矩变换$\sigma_l T$使得$\boldsymbol{y}$和$\boldsymbol{x}_1,\cdots,\boldsymbol{x}_k$都不动，而且$\boldsymbol{y}$与$\boldsymbol{x}_1,\cdots,\boldsymbol{x}_k$构成$T$的$k+1$个无关固定点。按此重复至多$4-k$次，即在$T$后面跟随至多$4-k$个反射后，便得到恒等变换，这等价于说$T$是至多$4-k$个反射的乘积。

定理 4.2.2 的证明 由引理4.2.2可知，等矩变换是反射之积。而使原点不动的等矩变换，其反射因子是过原点的直线所决定，即其反射必形如σ_k，σ_k是线性变换，T是线性变换之积。因而T是线性变换。

现在可以说，欧几里得几何实际上就是研究欧几里得空间在欧几里得群$E(3)$作用下图形的不变性质。

对于$\boldsymbol{a}\in\mathbb{R}^3$，考虑作用在$\mathbb{R}^3$上的变换$\mathscr{T}_a$，

$$\mathscr{T}_a:\ \boldsymbol{x}\to\boldsymbol{x}+\boldsymbol{a},\ \text{对所有}\ \boldsymbol{x}\in\mathbb{R}^3。$$

显然，$\mathscr{T}_a\in E(3)$。称$\mathscr{T}_a$为平移变换或**平移**。所有平移变换的集合，用$T(3)$表示，是$E(3)$的一个可换子群。

定理 4.2.3 (1) $T(3)\lhd E(3)$, $E(3)/T(3)\cong O(3)$。

(2) $E(3)=T(3)\rtimes O(3)$，即$E(3)$是$T(3)$和$O(3)$的半直积。

证明 (1) 设$\mathscr{T}\in T(3)$, $\mathscr{T}(\mathbf{0})=\boldsymbol{a}$，这里$\mathbf{0}$是零向量，也就是原点。那么$(\mathscr{T}_{-a}\cdot\mathscr{T})(\mathbf{0})=\mathbf{0}$。根据定理4.2.2，$\mathscr{T}_{-a}\cdot\mathscr{T}=\mathscr{A}\in O(3)$, $\mathscr{T}=\mathscr{T}_a\cdot\mathscr{A}$。为方便起见，将$\mathscr{T}$记为$\mathscr{T}=(\boldsymbol{a},\mathscr{A})$。由于$T(3)\cap O(3)=E$，$\mathscr{T}$的这种表法是唯一的。对于$O(3)$的任意给定的一个元素$\mathscr{B}$和$\mathbb{R}^3$的任意给定的一个元素$\boldsymbol{x}$，有

$$\begin{aligned}\mathscr{B}\mathscr{T}_a\mathscr{B}^{-1}(\boldsymbol{x})&=\mathscr{B}\mathscr{T}_a(\mathscr{B}^{-1}(\boldsymbol{x}))=\mathscr{B}(\mathscr{B}^{-1}(\boldsymbol{x})+\boldsymbol{a})\\&=\boldsymbol{x}+\mathscr{B}(\boldsymbol{a})=\mathscr{T}_{\mathscr{B}(a)}(\boldsymbol{x})。\end{aligned}$$

于是$\mathscr{B}\mathscr{T}_a\mathscr{B}^{-1}=\mathscr{T}_{\mathscr{B}(a)}\in T(3)$，这说明$T(3)\lhd E(3)$。考虑映射$\nu$: $E(3)\to O(3)$，它由$\nu((\boldsymbol{a},\mathscr{A}))=\mathscr{A}$给出。不难验证，$\nu$是同态映上，$\nu$的核$\operatorname{Ker}\nu=T(3)$，因此$E(3)/T(3)\cong O(3)$。

(2) 在(1)的证明过程中已经得到了(2)。进而给出半

直积乘法形式。这只需计算

$$(\boldsymbol{a},\mathscr{A})(\boldsymbol{b},\mathscr{B})(\boldsymbol{x})=(\boldsymbol{a},\mathscr{A})(\mathscr{B}(\boldsymbol{x})+\boldsymbol{b})$$
$$=\mathscr{A}\mathscr{B}(\boldsymbol{x})+\mathscr{A}\boldsymbol{b}+\boldsymbol{a}=(\boldsymbol{a}+\mathscr{A}\boldsymbol{b},\mathscr{A}\mathscr{B})\boldsymbol{x}。$$

由此得到

$$(\boldsymbol{a},\mathscr{A})(\boldsymbol{b},\mathscr{B})=(\boldsymbol{a}+\mathscr{A}\boldsymbol{b},\mathscr{A}\mathscr{B}),$$

这就是通常半直积的乘法形式。

令集合

$$O_a(3)=\{\mathscr{A}\in E(3)|\mathscr{A}\boldsymbol{a}=\boldsymbol{a}\},$$

显然，$O_a(3)$ 是$E(3)$ 的子群。若$\mathscr{A}\in O_a(3)$，那么

$$\mathscr{T}_a^{-1}\mathscr{A}\mathscr{T}_a(\boldsymbol{0})=\boldsymbol{0},$$

即$\mathscr{T}_a^{-1}\mathscr{A}\mathscr{T}_a\in O(3)$。于是有如下命题。

命题 4.2.1 $O_a(3)=\mathscr{T}_aO(3)\mathscr{T}_a^{-1}$，即 $O_a(3)$ 与正交群 $O(3)$ 通过 $\mathscr{T}_a$ 共轭。称 $O_a(3)$ 是关于点 $\boldsymbol{a}$ 的正交群（注意，这时将 $\boldsymbol{a}$ 看作空间中的点）。

由此结果得知，对于 $\mathscr{A}'\in O_a(3)$，必存在$\mathscr{A}\in O(3)$，使得 $\mathscr{A}'=\mathscr{T}_a\mathscr{A}\mathscr{T}_a^{-1}$。从几何直观来看，$\mathscr{A}'$是绕过点 $\boldsymbol{a}$ 的轴的转动或转动反演。确切地说，若$\mathscr{A}=C_k(\theta)$，那么，以通过点 $\boldsymbol{a}$（指向量 $\boldsymbol{a}$ 的端点）且与向量 $\boldsymbol{k}$ 平行的直线 l 为轴，将 $\boldsymbol{x}-\boldsymbol{a}$ 沿向量 $\boldsymbol{a}$ 平行移动到过 $\boldsymbol{a}$ 点，再将它绕 l 轴旋转 θ 角，就得到 $\mathscr{A}'_x$。这可由图 4-3 表之。

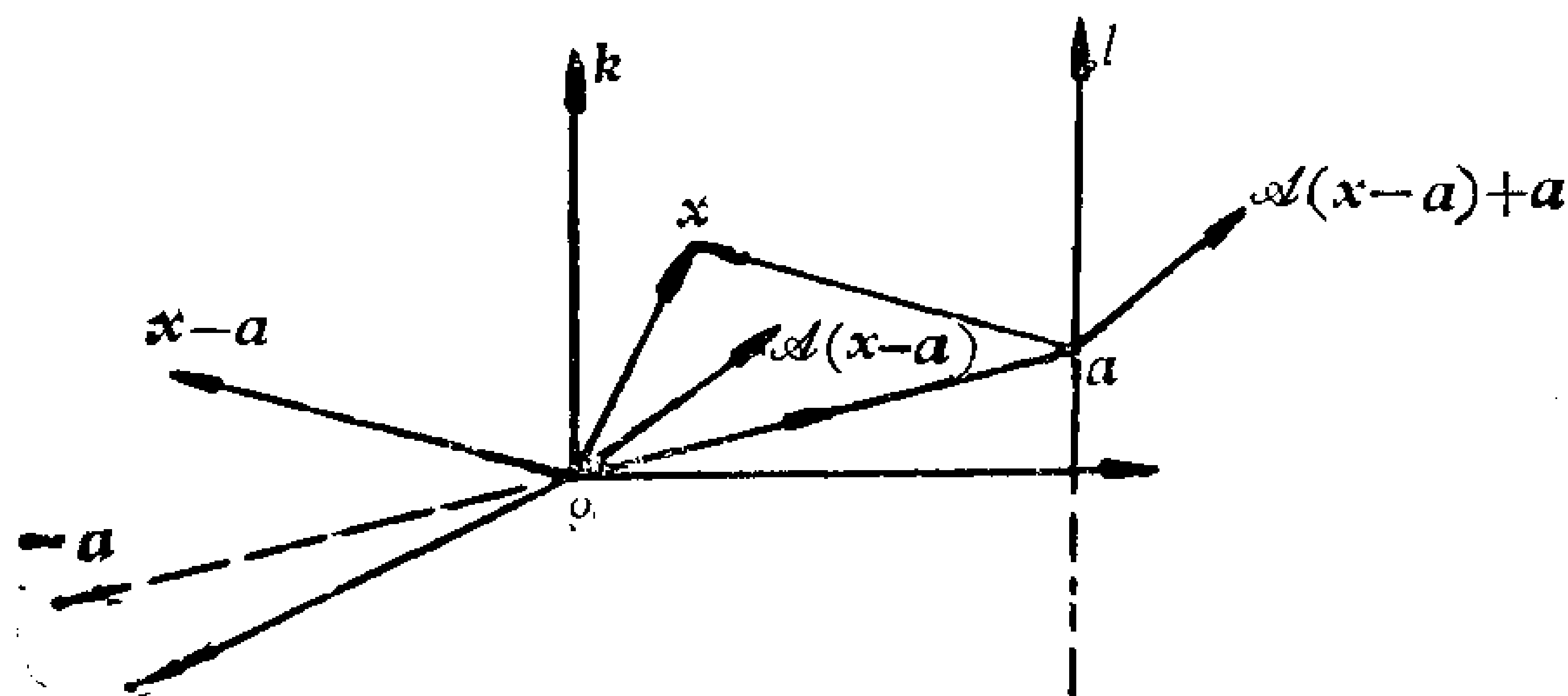


图 4-3

映射 $(\boldsymbol{a},\mathscr{A})\to\det\mathscr{A}$定义了$E(3)$ 到$\{1,-1\}$组成的 2 阶循环群 C_2 之上的一个同态，其核用$E(3)^+$表示，$E(3)^+=\{(\boldsymbol{a},$

$\mathscr{A})\in E(3)|\det\mathscr{A}=1\}$。$E(3)^+$就是物理学中熟知的**刚体运动群**，也称$E(3)^+$为正常欧几里得群。

§4.3 $E(3)$的离散子群

设S是空间$\mathbb{R}^3$的子集，集合

$$G_S=\{\mathscr{T}\in E(3)|\mathscr{T}S=S\}$$

是$E(3)$中将S映到S之上的所有变换的集合。显然，G_S是$E(3)$的一个子群，称G_S为S的**完全对称群**。而把G_S的子群称为S的**对称群**。这里S的对称群的定义与抽象对称群的定义是一致的。

例 4.3.1 $S=\mathbb{R}^3$，S的完全对称群$G_S=E(3)$。

例 4.3.2 $S=$中心在原点的单位球，$G_S=O(3)$。

例 4.3.3 $S=\{\boldsymbol{a}\}$，$G_S=\{E\}$。

集合S的对称群是反映它的对称性质，因而寻找所有可能的对称群的问题，不管是从几何学还是物理学的角度，乃至群论本身而言，都是一个十分重要的、有意义的问题。为此，首先需要对$E(3)$的子群进行分类。这是一个十分困难的问题。但在自然科学中经常出现的对称群只有两种类型：离散群和李群。这两类群在数学上各有处理的一套办法。由于篇幅的限制，本书不讨论李群，而只讨论有限离散群。对李群有兴趣的读者可参见参考文献〔11、12〕等等。

定义 4.3.1 **离散群**G是$E(3)$的一个子群，它满足性质：对于$\mathbb{R}^3$中任意给定的点$\boldsymbol{x}$和任意取定的球B_r，

$$B_r=\{\boldsymbol{y}\in\mathbb{R}^3|\ \|\boldsymbol{y}\|\leqslant r\},$$

在$\boldsymbol{x}$的G-轨道（参见§2.2）中只有有限个点包含在B_r中。

当然，$E(3)$的每个有限子群必定是离散群。再看几个例子。

例 4.3.4 $G=\{\mathscr{T}_a\in E(3)|\boldsymbol{a}=\sum_{i=1}^{3}a_i\boldsymbol{e}_i,\ a_i\in\mathbb{Z},\ i=1,2,3\}$是无限离散群。这里$\mathbb{Z}$是整数集合。

例 4.3.5 $G'=\{\mathscr{T}_a \in E(3) | a=\sum_{i=1}^{3} a_i e_i,\ a_i \in \mathbb{Q},\ i=1,2,3\}$不是离散群，这里$\mathbb{Q}$是有理数集合。这是因为具有形式$a=\sum_{i=1}^{3} a_i e_i$，$a_i \in \mathbb{Q}$，而且满足$\|x+a\|<r$的$a$有无穷多个，这意味着$x$的$G'$-轨道在球$B_r$中有无穷多个点。

例 4.3.6 $G=<C_k(\theta) | \theta=\frac{2\pi}{a},\ a$不是有理数$>$。$G$不是离散子群。事实上，对于$\mathbb{R}^3$中任意给定的点$x$，可选取$r$足够大（只要$r>\|x\|$），使得集合$G_x$包含在$B_r$之中。取$x \neq \alpha k$，$\alpha \in \mathbb{R}$，$C_k(\theta)l(x)$，$l=0,1,2,\cdots$，全不相同，但他们全包含在$B_r$之中。因此$G$不是离散群。

下边主要讨论有限范围集合S（即S可包含在一个充分大的球B_r之内）的离散对称群的性质。

定理 4.3.1 令S是$\mathbb{R}^3$中的非空的有限范围集合，G是S的离散对称群。那么至少存在一点$y \in \mathbb{R}^3$，使得G中每个元素g都有$gy=y$，即群G的所有元素至少有一个公共不动点。

证明 取$x \in S$，考虑包含x的G-轨道，即集合

$$G_x=\{g_x | g \in G\}。$$

设集合S包含在球B_r之中。由于G是S的对称群，有$G_x \subset S \subset B_r$。再根据$G$是离散解，集合$G_x \cap B_r = Gx$只有有限个点。设

$$G_x=\{x_1=x,\ x_2,\cdots,x_n\},$$

令$y=\frac{1}{n}\sum_{i=1}^{n} x_i$。证明$y$就是群$G$的公共不动点。实际上，任取$g \in G$，$gy=\frac{1}{n}\sum_{i=1}^{n} g x_i$。因为有$a \in \mathbb{R}^3$和$\mathscr{A} \in O(3)$，使得$g=\mathscr{T}_a \cdot \mathscr{A}$。由于$G$是有限范围$S$的对称群，取$z \in S$，它具性质：$\|z\|=\max\{\|x\| \ | x \in S\}$，要使得$gz \in S$，只能是$a=0$。

于是 $g\in O(3)$，是保持原点不动的线性变换，$g\left(\frac{1}{n}\sum_{i=1}^{n}\boldsymbol{x}_i\right)=\frac{1}{n}\sum_{i=1}^{n}g\boldsymbol{x}_i$，这正是所断言的。另外，不难看出，

$$\{g\boldsymbol{x}_1,\ g\boldsymbol{x}_2,\cdots,g\boldsymbol{x}_n\}=\{\boldsymbol{x}_1,\ \boldsymbol{x}_2,\cdots,\boldsymbol{x}_n\},$$

于是 $g\boldsymbol{y}=\boldsymbol{y}$，定理得证。

系 4.3.1 $E(3)$ 的任何一个有限子群 G 在 $\mathbb{R}^3$ 中都有一个公共不动点。

证明 取 $\mathbb{R}^3$ 中任意一点 $\boldsymbol{x}$，令 $S=G\boldsymbol{x}$，那么 G 是有限集合 S 的离散对称群。由定理 4.3.1 便得到本系。

定理 4.3.2 设 G 是 $E(3)$ 的离散子群，而且 G 的元素有公共不动点 $\boldsymbol{y}$，那么 G 是使点 $\boldsymbol{y}$ 固定的转动和转动反演构成的正交群 $O_y(3)$ 的一个有限子群。

证明 取球 B_r 是以 $\boldsymbol{y}$ 为球心、r 为半径的球。令 $\boldsymbol{x}_1$，$\boldsymbol{x}_2$，$\boldsymbol{x}_3$，$\boldsymbol{x}_4$ 是球 B_r 中不共面的 4 个点和 $g\in G$，$\|gx_i-y\|=\|gx_i-gy\|=\|x_i-y\|\leqslant r$，这表明 x_i 的 G-轨道 G_{x_i} 位于 B_r 之中。由于 G 是离散群，则有 $|G_{x_i}|<\infty$，即集合 $\{gx_i|\,g\in G\}=G_{x_i}$ 是有限集合。另一方面，若有 $h\in G$，使得 $gx_i=hx_i$，$i=1,2,3,4$，根据引理 4.2.1，有 $g=h$。即 g 被 g_{xi}，$i=1,2,3,4$ 这 4 点完全决定。于是 $|G|\leqslant|G_{x_1}||G_{x_2}||G_{x_3}||G_{x_4}|<\infty$，即 G 是有限群。定理的其余部分是显然的。

由定理 4.3.1 和定理 4.3.2，立即可以得到系 4.3.2。

系 4.3.2 有限物体 S 的离散对称群 G 总是一个有限群，它与 $O(3)$ 的一个有限子群 K 共轭。确切地说，$\mathscr{T}_yG\mathscr{T}_y^{-1}=K$，其中 $\mathscr{T}_y\in Б(3)$，$K\subset O(3)$，而且 K 是 $\mathscr{T}_y^{-1}S$ 的对称群。

对所有有限对象的离散对称群进行分类的问题，根据系 4.3.2 可归结为给出 $O(3)$ 的所有有限子群的问题。另一方面，在物理学上共轭对称性又是不可区分的，这表明定出 $O(3)$ 的有限子群是有实际意义的。$O(3)$ 的任意一个有限子群都有一个固定点，

所以称为**点群**。只含有转动的点群称为**第一类点群**，含有转动和转动反演的点群称为**第二类点群**。这二类点群之间的关系由下面定理给出。

定理 4.3.3 设G是$O(3)$的有限点群，而群$K=G\cap SO(3)$，即K是G的转动子群，那么群G和群K之间的关系只可能是下面3种情况之一：

（1）$G=K$；

（2）$G=K\cup IK$，其中I是反演变换；

（3）$G\neq K$，$I\notin G$和$G\cong G^{+}=K\cup K^{+}$，其中

$$K^{+}=\{Ig|\, g\in G\backslash K\}。$$

证明 考虑G到2阶循环群的映射det，det：$G\to C_2=\{1,-1\}$，映像det的核为K，$K\lhd G$。下边分两种情形讨论。

（a）$G=K$，那么G为第一类点群。这正是情形（1）。

（b）$G\neq K$，于是$[G:K]=2$，和

$$G=K\cup g_0K,$$

其中g_0是转动反演。

（i）若$I\in G$，则$I\in g_0K$，$IK=g_0K$，于是

$$G=K\cup IK。$$

G是第二类点群，这是情形（2）。

（ii）若$I\notin G$。设$G'=\{K,IK\}$，那么G'是第二类点群。令

$$K^{+}=\{Ig|\, g\in G\backslash K\},$$

容易看出，$K^{+}\cap K=\phi$，$|K^{+}|=|K|$。令

$$G^{+}=K\cup K^{+},$$

将证明$G^{+}\cong G$，这正是情形（3）。

首先，验证G^{+}成群，主要验证G^{+}对乘法运算封闭。事实上，G^{+}的元素总可表成$I^{\epsilon}g$，其中$g\in G$，和如果$g\in K$，$\epsilon=0$；如果$g\in K^{+}$，$\epsilon=1$。那末

$$I^{\epsilon_1}g_1\cdot I^{\epsilon_2}g_2=I^{\epsilon_1+\epsilon_2}g_1\cdot g_2。$$

如果$g_1\cdot g_2\in K$，即$\det(g_1g_2)=1$，则只可能是g_1，$g_2\in K$或者g_1，$g_2\notin K$，而这两种情况下均有$I^{\epsilon_1+\epsilon_2}=E$，于是$I^{\epsilon_1+\epsilon_2}g_1\cdot g_2\in$

$K\subset G^+$。如果 $g_1\cdot g_2\notin K$，$\det(g_1\cdot g_2)=-1$，那么有且只有一个 $g_i\notin K$。设 $g_1\notin K$，$g_2\in K$，于是 $I^{\varepsilon_1+\varepsilon_2}=I$，$g_1g_2\in G\setminus K$，即 $I^{\varepsilon_1+\varepsilon_2}g_1\cdot g_2\in K^+\subset G^+$。由此易知，$G^+$ 成群。考虑 G 到 G^+ 的映射 α：$G\rightarrow G^+$，$\alpha(g)=I^{\varepsilon}g$。易验证，$\alpha$ 是群同态映上，再由 $|G|=|G^+|$，得到 α 是群同构，即 $G\cong G^+$，定理得证。

由定理 4.3.3 可知，只要给出了所有的第一类点群，就可构造出所有的第二类点群，而且定理 4.3.3 的（3）给出了由第一类点群到第二类点群的非平凡构造。

下边，在进一步讨论点群之前，先通过正多面体的对称群给出一些具体的例子。

§4.4　正多面体和它们的对称群

中学的立体几何课本中就已经介绍了正多面体的定义、种类及构成。在这节，主要讨论正多面体的对称群。事实上，正多面体的对称群都是 3 维空间正交群 $O(3)$ 的有限子群，即都是点群。

回忆一下关于正多面体的知识。

首先需要等价的概念。在三维欧几里得空间中，二个图形 A_1 和 A_2 等价，当且仅当存在 $E(3)$ 中的一个元素 g，使得 $g(A_1)=A_2$，即指变换 g 作用在图形 A_1 上便得到 A_2。

所谓的正多面体指的是满足下面三个条件的一种凸多面体：

（i）多面体的表面都是一些彼此等价的正多边形；

（ii）多面体的角顶都等价；

（iii）多面体的棱边都等价。

设正多面体的所有面都是正 n 边形，在每个顶点相交的棱数都是 m，由于凸 m 面角的所有面角之和小于 2π，则下面的不等式成立：

$$\frac{m(n-2)\pi}{n}<2\pi。$$

由此不等式，再注意到 m 和 n 只能取正整数，而且 $m,n\geqslant 3$，得

到 n 和 m 的可能值（n，m）为：

n	3	3	3	4	5
m	3	4	5	3	3

再由著名的欧拉（Euler）公式：

$$面数+顶点数=棱数+2,$$

便可求出全部可能的正多面体。确切地说，若设 y 表示面数，x 表示顶点数，则有方程组：

$$\begin{cases} mx = ny \\ x + y = \dfrac{mx}{2} + 2 \end{cases}$$

此方程组的解：

(i) $(n, m) = (3, 3)$：$y = 4$，$x = 4$。

(ii) $(n, m) = (3, 4)$：$y = 8$，$x = 6$。

(iii) $(n, m) = (3, 5)$：$y = 20$，$x = 12$。

(iv) $(n, m) = (4, 3)$：$y = 6$，$x = 8$。

(v) $(n, m) = (5, 3)$：$y = 12$，$x = 20$。

于是，上面 (n, m) 的每一组值都唯一地决定了可能的一个正多面体，它们分别是：

(i) 正四面体。

(ii) 正八面体。

(iii) 正二十面体。

(iv) 正六面体。

(v) 正十二面体。

关于这 5 个正多面体的存在性，是大家熟知的。于是得到：有而且只有上面 5 个正多面体。

下面找每个正多面体的旋转对称群和完全对称群。一个物体 A 的旋转对称群是指集合

$$R(A) = \{g \in SO(3) \mid g(A) \sim A\},$$

其中 $g(A) \sim A$ 是指物体 A 被 g 作用后，得到的 $A_1 = g(A)$ 与

A，就它们在空间的位置和取向，是完全无法区分的。例如，位于平面σ上的一个正三角形A，绕过它的中心且垂直于平面σ的直线旋转π，得到的三角形与原来的正三角形A，就它们在空间中的位置和取向来看，完全无法区分。物体A的完全对称群是指集合

$$C(A)=\{g\in O(3)|g(A)\sim A\}。$$

显然，$R(A)$和$C(A)$分别是$SO(3)$和$O(3)$的子群。这两个群均称为**物体 A 的对称群**。(注意，这里对称群的定义与§4.3中给出的是一致的，但这里比较局限。) 由于$SO(3)$是由绕过原点的轴的旋转所组成，$O(3)$是由旋轴及旋轴反演所组成，因此要找A的对称群，只需找出全部满足$g(A)\sim A$的旋转及旋轴反演即可。

(1) 正四面体的对称群

对于正四面体$ABCD$，先选定直角坐标轴。取过边AD的中点和BC的中点的直线为z轴，过边AB的中点和DC的中点的直线为y轴，这两条直线的交点o为原点，过o作垂直于平面$y-z$的直线为x轴。

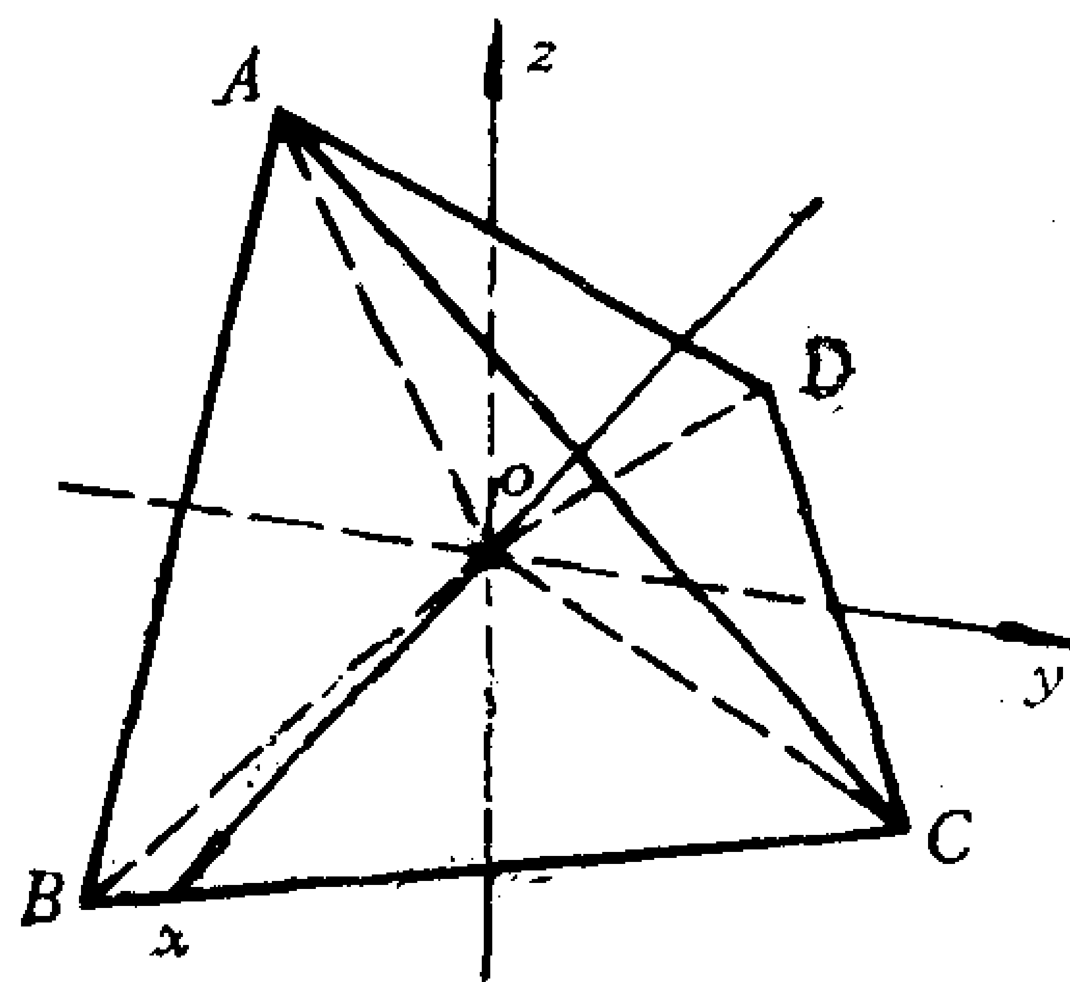


图 4-4

正四面体的所有可能的旋转是：

(i) 绕z轴旋转$180°$，即变换$C_{\mathbf{z}}(\pi)$，$\mathbf{z}$表示沿z轴的单位向量，其方向由图给出；

(ii) 绕y轴旋转$180°$，即$C_{\mathbf{y}}(\pi)$；

(iii) 绕x轴旋转$180°$，即$C_{\mathbf{x}}(\pi)$；

(iv) 以过点A和原点o的直线为轴转$\frac{2\pi}{3}$和$\frac{4}{3}\pi$，即$C_{oA}\left(\frac{2\pi}{3}\right)$和$C_{oA}\left(\frac{4}{3}\pi\right)$；

(v) 以过点B和原点o的直线为轴转$\frac{2\pi}{3}$和$\frac{4}{3}\pi$，即

$C_{oB}\left(\frac{2\pi}{3}\right)$ 和 $C_{oB}\left(\frac{4}{3}\pi\right)$;

(vi) 以过点 C 和原点 o 的直线为轴转 $\frac{2\pi}{3}$ 和 $\frac{4}{3}\pi$，即 $C_{oC}\left(\frac{2\pi}{3}\right)$ 和 $C_{oC}\left(\frac{4}{3}\pi\right)$;

(vii) 以过点 D 和原点 o 的直线为轴转 $\frac{2\pi}{3}$ 和 $\frac{4}{3}\pi$，即 $C_{oD}\left(\frac{2\pi}{3}\right)$ 和 $C_{oD}\left(\frac{4}{3}\pi\right)$;

(viii) 单位变换 E。

以上这12个元素组成了正四面体的旋转对称群，用 T 表示该群。T 的共轭类是：

$$E,\ 3C_2,\ 8C_3。$$

这里 $3C_2$，表示由 3 个旋转角为 $\frac{2\pi}{2}$ 的旋转变换组成一个共轭类，$8C_3$ 是指此共轭类由 8 个旋转角为 $\frac{2\pi}{3}$ 的旋转组成。以后也用此法来表示共轭类。

正四面体所有可能的旋转反演是：

(i) 绕 z 轴的旋转反演 $S_z\left(\frac{\pi}{2}\right)$，$S_z\left(\frac{\pi}{2}\right)^2=C_z(\pi)$，$S_z\left(\frac{\pi}{2}\right)^3=S_z\left(\frac{3}{2}\pi\right)$;

(ii) 绕 y 轴的旋转反演 $S_y\left(\frac{\pi}{2}\right)$，$S_y\left(\frac{\pi}{2}\right)^2=C_y(\pi)$，$S_y\left(\frac{\pi}{2}\right)^3=S_y\left(\frac{3}{2}\pi\right)$;

(iii) 绕 x 轴的旋转反演 $S_x\left(\frac{\pi}{2}\right)$，$S_x\left(\frac{\pi}{2}\right)^2=C_x(\pi)$，$S_x\left(\frac{\pi}{2}\right)^3=S_x\left(\frac{3}{2}\pi\right)$;

(iv) 分别过下面 6 个平面的反映 $\sigma_1,\sigma_2,\cdots,\sigma_6$: OBC, OBD,

OBA，OCD，OCA，ODA。

以上这 24 个元素组成了正四面体的完全对称群，用 T_d 表示该群。T_d 的共轭类是：

$$E,\ 8C_3,\ 3C_2,\ 6S_4,\ 6\sigma,$$

这里 $6S_4$ 是指这个共轭类由 6 个转角为 $\frac{2\pi}{4}$ 的旋转反演组成，6σ 是指共轭类由 6 个反映组成。

（2）正八面体的对称群

先选定坐标轴。令过相对顶点的三条直线分别为 3 个坐标轴，如图 4-5 所示，其交点 o 为坐标原点。

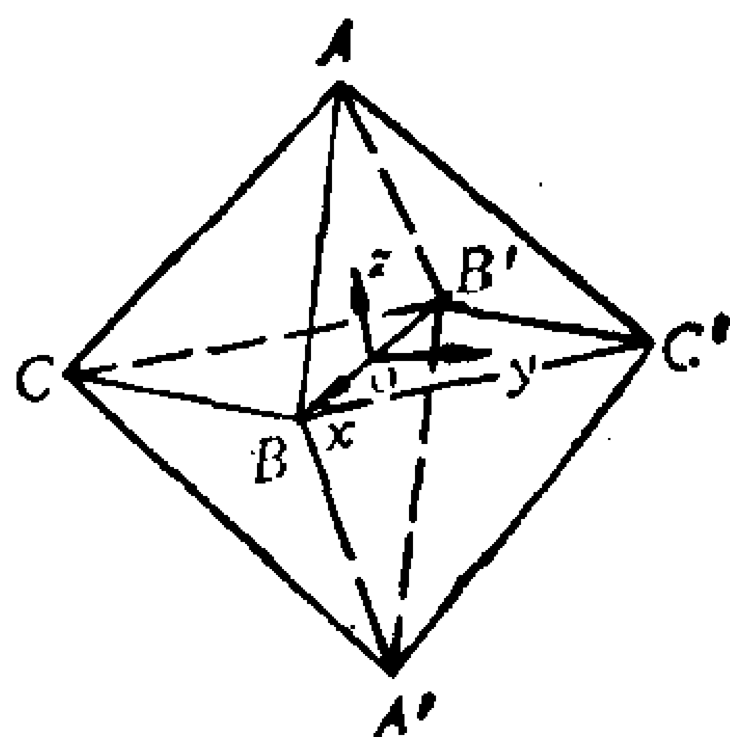


图 4-5

正八面体所有可能的旋转是：

（i）分别以 AA'，BB'，CC' 为轴旋转 $\frac{\pi}{2}$，这些变换是 $C_z\left(\frac{\pi}{2}\right)$，$C_y\left(\frac{\pi}{2}\right)$，$C_x\left(\frac{\pi}{2}\right)$。进而由它们生成的变换是 $C_z(\pi)$，$C_z\left(\frac{3}{2}\pi\right)$，$C_y(\pi)$，$C_y\left(\frac{3}{2}\pi\right)$，$C_x(\pi)$，$C_x\left(\frac{3}{2}\pi\right)$。

（ii）设过相对棱边中点的直线分别为 l_1，l_2，…，l_6。分别以 $l_1, l_2, \cdots, l_6$ 为轴旋转 π，得到变换 $C_{l_1}(\pi), C_{l_2}(\pi), \cdots, C_{l_6}(\pi)$。

（iii）设过相对三角形表面的中心的直线分别为 l'_1，l'_2，l'_3，l'_4。分别以 l'_1, l'_2, l'_3, l'_4 为轴旋轴 $\frac{2}{3}\pi$，得到变换 $C_{l'_1}\left(\frac{2}{3}\pi\right)$，…，$C_{l'_4}\left(\frac{2}{3}\pi\right)$。进而由它们生成的变换是 $C_{l'_1}\left(\frac{4}{3}\pi\right)$，…，$C_{l'_4}\left(\frac{4}{3}\pi\right)$。

（iv）单位变换。

以上这 24 个元素是正八面体的所有可能的旋轴对称变换，它们组成 24 阶旋转对称群，用 O 表示该群。O 的共轭类是：

$$E,\ 6C_4,\ 9C_2,\ 8C_3。$$

正八面体所有可能的旋转反演是：

（ i ）分别以直线 AA'，BB'，CC' 为轴旋转 $\frac{\pi}{2}$ 的旋轴反演及它们生成的元素：

$$S_z\left(\frac{\pi}{2}\right),\ S_z(\pi)=C_z(\pi),\ S_z\left(\frac{3}{2}\pi\right),$$

$$S_y\left(\frac{\pi}{2}\right),\ S_y(\pi)=C_y(\pi),\ S_y\left(\frac{3}{2}\pi\right),$$

$$S_x\left(\frac{\pi}{2}\right),\ S_x(\pi)=C_x(\pi),\ S_x\left(\frac{3}{2}\pi\right),\ E。$$

（ii）以 l_1'，l_2'，l_3'，l_4' 为轴的旋轴反演及它们生成的元素：

$$S_{l_1'}\left(\frac{2\pi}{3}\right),\ \cdots,\ S_{l_4'}\left(\frac{2\pi}{3}\right),$$

$$S_{l_1'}\left(\frac{4}{3}\pi\right)=C_{l_1'}\left(\frac{4}{3}\pi\right),\cdots,S_{l_4'}\left(\frac{4}{3}\pi\right)=C_{l_4'}\left(\frac{4}{3}\pi\right),$$

$$I,\ C_{l_1'}\left(\frac{1}{3}\pi\right)^2,\ \cdots,\ C_{l_4'}\left(\frac{1}{3}\pi\right)^2,$$

$$S_{l_1'}\left(\frac{2}{3}\pi\right)^5\cdots,S_{l_4'}\left(\frac{2}{3}\pi\right)^5,\ E。$$

这里 I 是反演变换。

（iii）以 o 为反演中心的反演 I，$I=S_{l_1'}\left(\frac{2}{3}\pi\right)^3$。

（iv）分别对下面 3 个平面的反射（参见系 4.1.1 下面）σ_1，σ_2，σ_3：

$$ABA'B',\ CBC'B',\ ACA'C'。$$

（v）通过两个顶点并且平分一对相对棱边的平面有 6 个。设这 6 个平面分别为 σ_1'，σ_2'，$\cdots$，σ_6'（请读者自己列出这六个平面）。相对这 6 个平面的反射仍用 σ_1'，$\cdots$，σ_6' 表示。

将上面得到的变换去掉旋转变换及重复的，剩下的 24 个变换就是全部旋转反演变换。

以上这 48 个元素组成了正八面体的完全对称群，用 O_h 表示

该群，按共轭类列出为：

$$E, \quad I, \quad 6C_4, \quad 9C_2, \quad 8C_3, \quad 6\bar{S}_4, \quad 8\bar{S}_6, \quad 3\sigma_h, \quad 6\sigma_d。$$

（3）正二十面体的对称群

选定坐标系。连结相对顶点 A 和 A' 得线段 AA'，取此线段的中心作为坐标原点，过 oA 的直线取为 z 轴，在过原点垂直于 z 轴的平面上选 x 轴和 y 轴，使之成为直角坐标系。

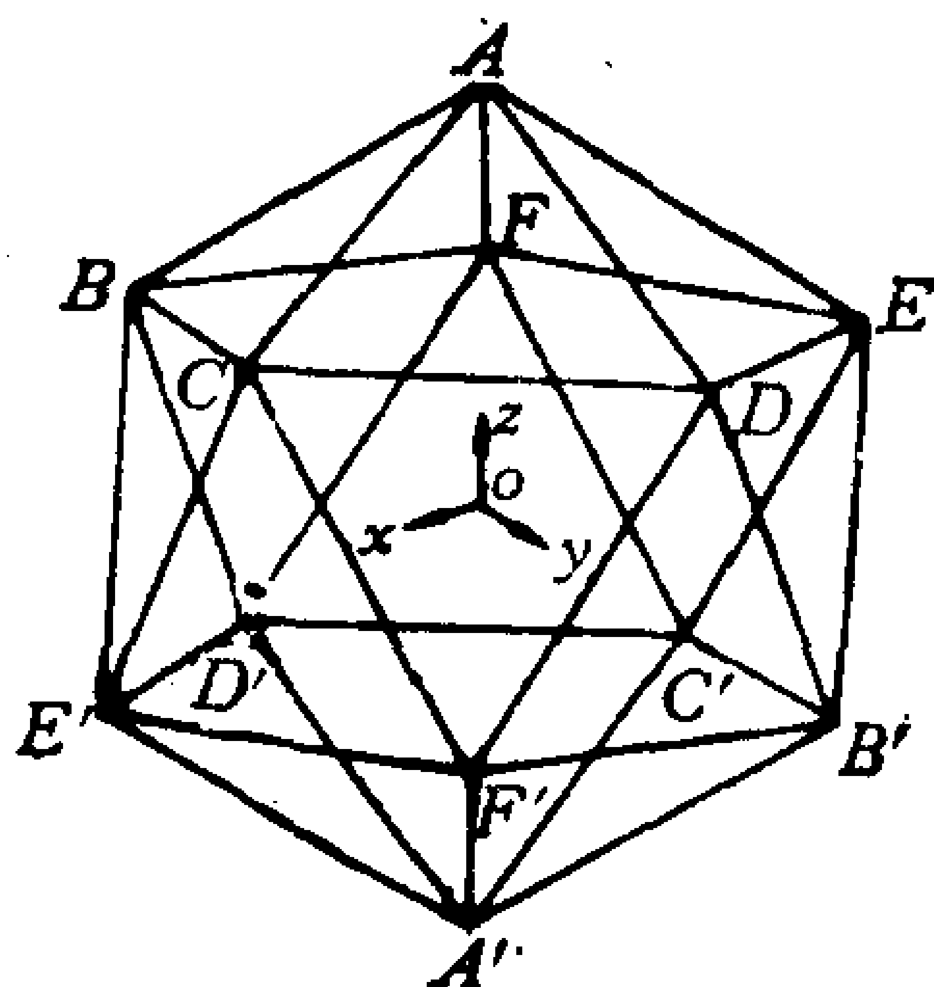


图 4-6

正二十面体所有可能的旋转是：

（i）过 AA'，BB'，CC'，DD'，EE'，FF' 的直线分别用 l_1，l_2，…，l_6 表示。分别以 l_1，…，l_6 为轴旋转 $\frac{2\pi}{5}$ 的变换，及它们生成的变换是：

$$C_{l_1}\left(\frac{2}{5}\pi\right)^i, C_{l_2}\left(\frac{2}{5}\pi\right)^i, \quad \cdots, C_{l_6}\left(\frac{2}{5}\pi\right)^i,$$

$$i = 1, 2, 3, 4。$$

(ii) 过相对表面中心的直线有 10 条。例如过面 ACD 的中心和面 $A'C'D'$ 的中心的直线，分别用 k_1，k_2，…，k_{10} 表示这 10 条直线。以 k_1，…，k_{10} 为轴旋转 $\frac{2}{3}\pi$ 的旋转变换，它们生成的变换是：

$$C_{k_i}\left(\frac{2}{3}\pi\right)^j, \quad i = 1, 2, \cdots, 10, \quad j = 1, 2。$$

(iii) 过相对棱边中点的直线有 15 条。例如过棱边 AC 的中点和 $A'C'$ 的中点的直线，分别用 m_1，m_2，…，m_{15} 表示这 15 条直线。以 m_1，m_2，…，m_{15} 为轴转 π 的旋转变换和它们生成的变换是：

$$C_{m_j}(\pi), \quad j = 1, 2, \cdots, 15; \quad E。$$

(iv) 单位变换 E。

以上这 60 个旋转变换是正二十面体所有可能的旋转对称，它们组成 60 阶旋轴对称群，用Y表示该群。按共轭类列出为：

$$E,\ 12C_5,\ 12C_5^2,\ 20C_3,\ 15C_2$$

注意，$C_{l_i}\left(\frac{2}{5}\pi\right)$ 与 $C_{l_i}\left(\frac{2}{5}\pi\right)^4$ 共轭，$C_{l_i}\left(\frac{2}{5}\pi\right)^2$ 与 $C_{l_i}\left(\frac{2}{5}\pi\right)^3$ 共轭。

正二十面体的所有可能的旋转反演是：

（v）分别以l_1，l_2，…，l_6（参见（i））为轴的旋转反演 $S_{l_f}\left(\frac{\pi}{5}\right)^j$，$f=1, 2, \cdots, 6$，$j=1, 3, 5, 7, 9$。其中 $S_{l_f}\left(\frac{\pi}{5}\right)^5=i$，这里$i$是反演。

（vi）分别以k_1，k_2，…，k_{10}（参见（ii））为轴的旋转反演是 $S_{k_f}\left(\frac{2\pi}{6}\right)^j$，$f=1, 2, \cdots, 10$，$j=1, 3, 5$。其中 $S_{k_f}\left(\frac{2}{6}\pi\right)^3=I$。

（vii）有 15 个反映平面，其中每个反映平面过一对相对棱边。例如过$CDC'D'$的平面，用σ_1，σ_2，…，σ_{15}表示由这 15 个反映平面决定的反映。

以上这 120 个变换是正二十面体的全部旋转和旋转反演，它们构成了正二十面体的完全对称群，用Y_h表示该群。共轭类列出为：

$$E, 12C_5, 12C_5^2, 20C_3, 15C_2, 12S_{10}, 12S_{10}^3, 20S_6, I, 15\sigma。$$

其中C_5^2是指绕某轴旋转$\frac{2\pi}{5}$这一旋转变换的平方，余类推。

正六面体的对称群与正八面体相同。事实上，若将正六面体的每两个相邻面的中心联结起来就得到一个正八面体。另一方面，将正八面体的相邻面的中心联结起来就得到一个正六面体。由于$O(3)$中的变换是线性的，保长的一一映射，因此正六面体与正八面体有相同的对称群。

正二十面体的对称群与正十二面体的对称群相同。将正二十面体的每两个相邻面的中心联结起来就得到一个正十二面体。反之，正十二面体的每个面的中心可构成正二十面体的十二个顶点。

到现在为止，定出了正多面体的所有的旋转对称群和完全对称群。

§4.5 第一类点群

第一类点群都是有限旋转群，即是 $O^+(3)=SO(3)$ 的有限子群。

设 G 是 $SO(3)$ 的有限子群，M 是以原点 o 为中心的单位球的球面。G 的元素显然把 M 映射到 M 之上。M 上的一点 $\boldsymbol{x}$，如果对于 G 中某一个非单位元 $g(\neq e)$ 有性质：$g\boldsymbol{x}=\boldsymbol{x}$，则称 $\boldsymbol{x}$ 为**极点**。由于 $G\subset SO(3)$，除单位元外，G 的每个元素都有两个极点，它们是其旋转轴与 M 的交点。令 S 是 M 上相对群 G 的所有极点的集合，即

$$S=\{\boldsymbol{x}\in M\mid \exists g\in G,\ g\neq e,\ \text{使得} g\boldsymbol{x}=\boldsymbol{x}\}。$$

若 $\boldsymbol{x}\in S$，$g\in G$，那么 $g\boldsymbol{x}\in S$，即群 G 可看作集合 S 上的置换群。事实上，由 $\boldsymbol{x}\in S$，存在 $g_1\in G$，$g_1\neq e$，使得 $g_1\boldsymbol{x}=\boldsymbol{x}$。于是 $(gg_1g^{-1})(g\boldsymbol{x})=g\boldsymbol{x}$，和 $gg_1g^{-1}\neq e$，即 $g\boldsymbol{x}$ 是由 gg_1g^{-1} 决定的极点。

令

$$W=\{(g,\boldsymbol{v})\mid g\in G,\ g\neq e,\ \boldsymbol{v}\in S \text{和} g\boldsymbol{v}=\boldsymbol{v}\},$$

对于 $\boldsymbol{v}\in S$，令

$$G(\boldsymbol{v})=\{g\boldsymbol{v}\mid g\in G\},$$

即 $G(\boldsymbol{v})$ 是包含点 $\boldsymbol{v}$ 的 G 轨道。令

$$G^{\boldsymbol{v}}=\{g\in G\mid g\boldsymbol{v}=\boldsymbol{v}\},$$

$G^{\boldsymbol{v}}$ 是点 $\boldsymbol{v}$ 的固定子群。有

$$|G|=|G(\boldsymbol{v})|\cdot|G^{\boldsymbol{v}}|,$$

其中 $|G|$ 表示集合 G 的元素个数，和

$$|W|=2(|G|-1)。$$

若S在G的作用下分成k个轨道，取$\{v_1, v_2, \cdots, v_k\}$为$k$个轨道的代表元集合。令$m_i=|G(v_i)|$，$n_i=|G^{v_i}|$，即$m_i$是包含$v_i$的轨道的元素个数，$n_i$是$v_i$的固定子群的阶。若$v\in G(v_i)$和$gv_i=v$，那么$g^{-1}G^v g=G^{v_i}$，这表明同一轨道上的两个点的固定子群是共轭的，以及$|G^v|=|G^{v_i}|$。再考虑$|W|$，有

$$|W|=\sum_{v\in S}(|G^v|-1)=\sum_{i=1}^{k}m_i(|G^{v_i}|-1)$$

$$=\sum_{i=1}^{k}m_i(n_i-1)。$$

注意，对每个i，有$m_i\cdot n_i=|G|$。于是得到

$$2(|G|-1)=\sum_{i=1}^{k}(|G|-m_i),$$

即

$$2\left(1-\frac{1}{|G|}\right)=\sum_{i=1}^{k}\left(1-\frac{1}{n_i}\right) \tag{4-7}$$

于是

$$\sum_{i=1}^{k}\left(1-\frac{1}{n_i}\right)<2。$$

不失一般性，可设$|G|>1$（否则，G是平凡的），那么对每个i，$n_i\geqslant 2$。有

$$\frac{1}{2}\leqslant 1-\frac{1}{n_i}<1,$$

于是

$$\frac{k}{2}\leqslant\sum_{i=1}^{k}\left(1-\frac{1}{n_i}\right)<2,$$

由此得到$k<4$。这表明S在G作用下至多有3个轨道。下边，就k的可能值分别进行讨论。

（1）$k=1$，由式(4-7)有

$$1 \leqslant 2\left(1-\frac{1}{|G|}\right)=1-\frac{1}{n_1},$$

这不可能。因此，只可能是 $k=2$ 或 $k=3$。

（2）$k=2$，由式(4-7)有

$$2-\frac{2}{|G|}=1-\frac{1}{n_1}+1-\frac{1}{n_2}=2-\left(\frac{1}{n_1}+\frac{1}{n_2}\right),$$

即

$$2=|G|\left(\frac{1}{n_1}+\frac{1}{n_2}\right)=m_1+m_2。$$

由于对每个 i，显然有 $m_i \geqslant 1$，于是 $m_1=m_2=1$。这表明在 $k=2$ 时，每个轨道只有一个元素，$S=\{\boldsymbol{v}_1,\boldsymbol{v}_2\}$，而且 $\boldsymbol{v}_2=-\boldsymbol{v}_1$，群 G 的每个元素都使 $\boldsymbol{v}_1$ 和 $-\boldsymbol{v}_1$ 不动。据此和下面的引理，群 G 可完全确定。

引理4.5.1 令 $\boldsymbol{v}\in S$，那么群 G 中以 $\boldsymbol{v}$ 和 $-\boldsymbol{v}$ 为极点的所有旋转的集合是一个循环群。

证明 令集合

$$H=\{g\in G|g\boldsymbol{v}=\boldsymbol{v}\}\subset G,$$

显然 H 是 G 的一个子群。设 H 的元素为

$$H=\{e=h_1,\ h_2,\ \cdots,\ h_l\},$$

由于 $H\subset SO(3)$，H 的元素可表为 $h_i=C_v(\alpha_i)$，$1\leqslant i\leqslant l$。不失一般性，设 $\alpha_i\geqslant 0$，α_2 是最小旋转角。那么对每个 i，必有整数 k_i，使得 $\alpha_i=k_i\alpha_2$。因为对每个 i，存在整数 k_i，使得 $\alpha_i=k_i\alpha_2+\beta$，$0\leqslant\beta<\alpha_2$。由此，$h_i=C_v(k_i\alpha_2+\beta)=C_v(\alpha_i)^{k_i}C_v(\beta)$，$C_v(\beta)\in H$。这与 α_2 的选取相矛盾，除非 $\beta=0$。引理得证。

由此引理可知，在 $k=2$ 时，群 G 是有限循环群。

注意，G^v 实际上是 G 的以 $\boldsymbol{v}$ 为极点的所有旋转构成的循环群。通常用 $o(\boldsymbol{v})=|G^v|$ 表示极点 $\boldsymbol{v}$ 和 $-\boldsymbol{v}$ 的重数。实际上，$\boldsymbol{v}$ 被且只被 $o(\boldsymbol{v})$ 个旋转所固定。这便是重数一词的来源。

引理4.5.1可以重新叙述为：群 G 中以 L 为轴的所有旋转的集合成一循环群。若此群的阶是 n，称轴 L 为 n 阶轴，通常用 $L(n)$ 表示。

引理4.5.2 若两个极点v_1和$-v_1$在同一轨道，$g\in SO(3)$，$g(v_1)=-v_1$，那么g的旋转轴l垂直于v_1，旋转角为π，即$g=C_l(\pi)$，其中$l\perp v$。

证明 选定坐标，使g有矩阵表示

$$\begin{pmatrix}\cos\alpha & -\sin\alpha & 0\\ \sin\alpha & \cos\alpha & 0\\ 0 & 0 & 1\end{pmatrix},$$

z坐标由l给出。在此坐标下，$v=(x_1,x_2,x_3)$。由$gv=-v$，有

$$\begin{pmatrix}\cos\alpha & -\sin\alpha & 0\\ \sin\alpha & \cos\alpha & 0\\ 0 & 0 & 1\end{pmatrix}\begin{pmatrix}x_1\\ x_2\\ x_3\end{pmatrix}=\begin{pmatrix}-x_1\\ -x_2\\ -x_3\end{pmatrix},$$

由此解得$x_3=0$，这表明$l\perp v$；$\cos\alpha=-1$，这表明$\alpha=\pi$。引理得证。

（3）$k=3$，由式(4-7)得到

$$2\left(1-\frac{1}{|G|}\right)=3-\frac{1}{n_1}-\frac{1}{n_2}-\frac{1}{n_3},$$

即

$$1+\frac{2}{|G|}=\frac{1}{n_1}+\frac{1}{n_2}+\frac{1}{n_3},\quad |G|\geqslant n_i\geqslant 2 \qquad (4\text{-}8)$$

下面求满足式(4-8)的(n_1,n_2,n_3)。不失一般性，假设$n_1\leqslant n_2\leqslant n_3$。

（a）$n_1\geqslant 3$，由式(4-8)得到

$1+\frac{2}{|G|}\leqslant 1$，这不可能。因此，$n_1=2$。

（b）$n_1=2$，$n_2\geqslant 4$，由式(4-8)得到

$$\frac{1}{2}+\frac{2}{|G|}=\frac{1}{n_2}+\frac{1}{n_3}\leqslant\frac{1}{2},$$

这不可能。于是$2\leqslant n_2\leqslant 3$。

（c）$n_1=2$，$n_2=2$，由式(4-8)得到

$$\frac{2}{|G|}=\frac{1}{n_3},\quad n_3=\frac{|G|}{2}。$$

这表明$|G|\geqslant 4$和$|G|$是偶数。令$|G|=2n$，$n\geqslant 2$，有

$$'(n_1, n_2, n_3) = \left(2, 2, n = \frac{|G|}{2}\right)。$$

(d) $n_1 = 2$, $n_2 = 3$,

由式(4-8)得到

$$\frac{1}{6} + \frac{2}{|G|} = \frac{1}{n_3}, \quad 3 \leqslant n_3 < 6。 \qquad (4\text{-}9)$$

于是 n_3 的可能值是 3, 4, 5。

(i) $n_3 = 3$, $|G| = 12$;

(ii) $n_3 = 4$, $|G| = 24$;

(iii) $n_3 = 5$, $|G| = 60$。

综上所述，对于 $k = 3$，已得到第一类点群必定满足下列条件之一：

① $n_1 = n_2 = 2$, $n_3 = \frac{|G|}{2}$, $|G| \geqslant 4$;

② $n_1 = 2$, $n_2 = n_3 = 3$, $|G| = 12$;

③ $n_1 = 2$, $n_2 = 3$, $n_3 = 4$, $|G| = 24$;

④ $n_1 = 2$, $n_2 = 3$, $n_3 = 5$, $|G| = 60$。

下面证明，从①～④的每种情况都唯一地（在同构的意义下）确定了一个第一类点群。

① $n_1 = n_2 = 2$, $n_3 = \frac{|G|}{2}$, $|G| \geqslant 4$。

令 $|G| = 2m$，$m \geqslant 2$ 的整数，于是 $n_3 = m$。这表明有一个轨道只包含 2 个元素，取其一代表元为 x_3，则 $|G^{\vec{x}_3}| = m$。根据引理 1.5.1，$G^{\vec{x}_3}$ 是 m 阶循环群，它由绕固定轴 L（L 过 x_3），转角为 $\frac{2\pi}{m}$ 的转动 $C_{\vec{x}_3}\left(\frac{2\pi}{m}\right)$ 生成。再分两种情况讨论。

ⓐ $m > 2$

这时，L 的两个极点 x_3 和 $-x_3$ 在同一轨道。因为由 $n_1 = n_2 = 2$，不含 x_3 的另外二个轨道上每个极点的固定子群的阶都是 2，$2 \neq m$。不含 x_3 的两个轨道各有 m 个 2 重极点，有 m 个 2 阶转动轴 l_1, l_2, …, l_m 通过这 $2m$ 个极点。由这 m 个转轴决定的转

动$C_{l_i}(\pi)$，$i=1,2,\cdots,m$，将使x_3和$-x_3$相互交换，那么根据引理4.5.2，转轴l_i皆在过原点垂直于L的平面内；另一方面，绕L轴的转动$C_L\left(\frac{2\pi}{m}\right)$将轴$l_1$，$l_2$，…，$l_m$仍映射为它们自身，即引起这$m$个2阶轴的一个置换。由此可知，两个相邻的二阶轴之间的夹角$\theta=\frac{2\pi}{m}$，见图4-7。

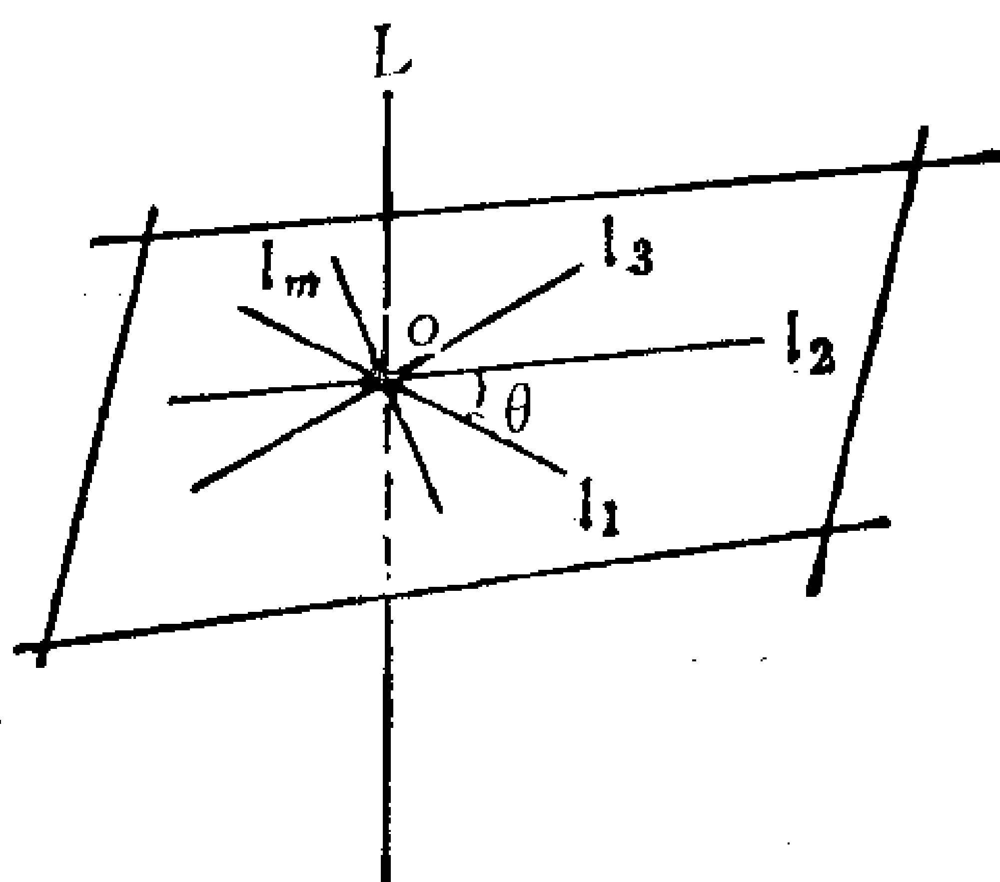


图 4-7

现在可以唯一地决定对应①的点群的结构。令$a=C_L\left(\frac{2\pi}{m}\right)$，$b=C_{l_1}(\pi)$。$C_m=\langle a\rangle$，即$C_m$是$a$生成的$m$阶循环群；$C_2=\langle b\rangle$，即$b$是2阶元。由于$|G|=2m$，有$[G:C_m]=2$，于是$C_m$是$G$中正规子群。由于$ba$将使$L$的两个极点互换，同时有两个不动点，根据引理4.3.1，$(ba)^2=e$，即$bab^{-1}=a^{-1}$。于是，群G是正规子群C_m和子群C_2的半直积，即$G=C_m\rtimes C_2$，群G的表现可由

$$G=\langle a,b\,|\,a^m=b^2=e,\ bab^{-1}=a^{-1}\rangle$$

给出。这正是前面已讲过的$2m$阶的二面体群D_m。

ⓑ　$m=2$

这时$|G|=4$。G不可能是4阶循环群。因此$G=D_2=K_4$，这里K_4是克莱因4元群。这与上面的结果一致。

综上讨论，对于情形①，群G同构于二面体群，即$G\cong D_m$。

进而，对于每一个m，都存在一个物体，D_m是由它的所有旋转对称组成的群。事实上，以正m边多边形为底，而其高不等于多边形边长的m棱柱体，就满足上面条件。同时，D_m也是平面上正m边形的所有对称（包括旋转和反映）所组成的群。然而，在平面上，相对某条直线的反映可通过空间中的旋转来实现。例如，当$m=5$，轴L垂直于正五边形所在平面而且通过中心，5

个2阶轴分别通过5个顶点，相邻夹角为$\frac{2\pi}{5}$。那么将正五边形看作空间中的图形，它的所有旋转对称组成D_5。见图4-8。

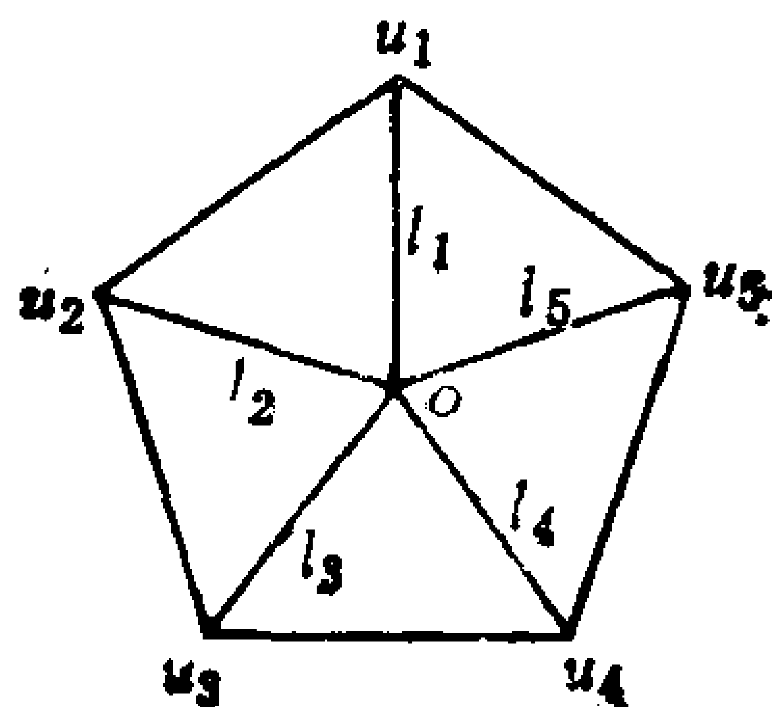


图 4-8

② $n_1=2$，$n_2=n_3=3$，$|G|=12$。

这时有二个轨道，每个均有4个极点，每个极点是三重的，即过这极点的轴是3阶的。还有一个轨道有6个极点，每个极点是2阶的。因此，群G有4个3阶轴$L_1,\cdots,L_4$和3个2阶轴。设$S'=\{x_1,x_2,x_3,x_4\}$是同一轨道上的4个极点，那么群G在S'上是可迁的。对于不同的i，j，k，存在$g\in G$，满足$gx_i=x_i$，$gx_j=x_k$。因为对于$g\neq e$，g只有二个不动点。由此，g把线段$[x_i,x_j]$映为线段$[x_i,x_k]$。g是保长变换，于是$\|x_i-x_j\|=\|x_i-x_k\|$。到此我们可知，x_1，x_2，x_3，x_4构成空间中正四面体的4个顶点。因此，G是四面体的旋转对称群T（见§4.4)的子群。进而，由$|G|=|T|=12$，得到$G=T$。

③ $n_1=2$，$n_2=3$，$n_3=4$，$|G|=24$。

解③对应着4个3阶轴，3个4阶轴和6个2阶轴。设3个4阶轴为L_1，L_2，L_3，与它们相关的6个极点x_1，x_2，$\cdots$，x_6构成一个轨道。G对此轨道上极点的作用是非平凡的和可迁的。设L_1包含的两个极点是x_1和x_2，以L_1为轴的4阶循环群为D_4。对于$g\in C_4$，有$gx_i=x_i$，$i=1$，2，和$gx_j=x_k$，$3\leqslant j,k\leqslant 6$，$j\neq k$。于是$g$把线段$[x_1,x_j]$映到$[x_1,x_k]$，$[x_2,x_j]$映到$[x_2,x_k]$。由于$g$是保长变换，有$\|x_i-x_j\|=\|x_i-x_k\|$，$i=1$，2。因此，不在同一轴上的两个极点之间的距离都相等。由初等几何的知识不难看出，三个轴L_1，L_2，L_3必定是互相垂直的。现构造立方体C，使得这6个极点为C的六个面的中心，进而将立方体C的相邻面的中心联結起来就得到一个正八面体。见图4-9。

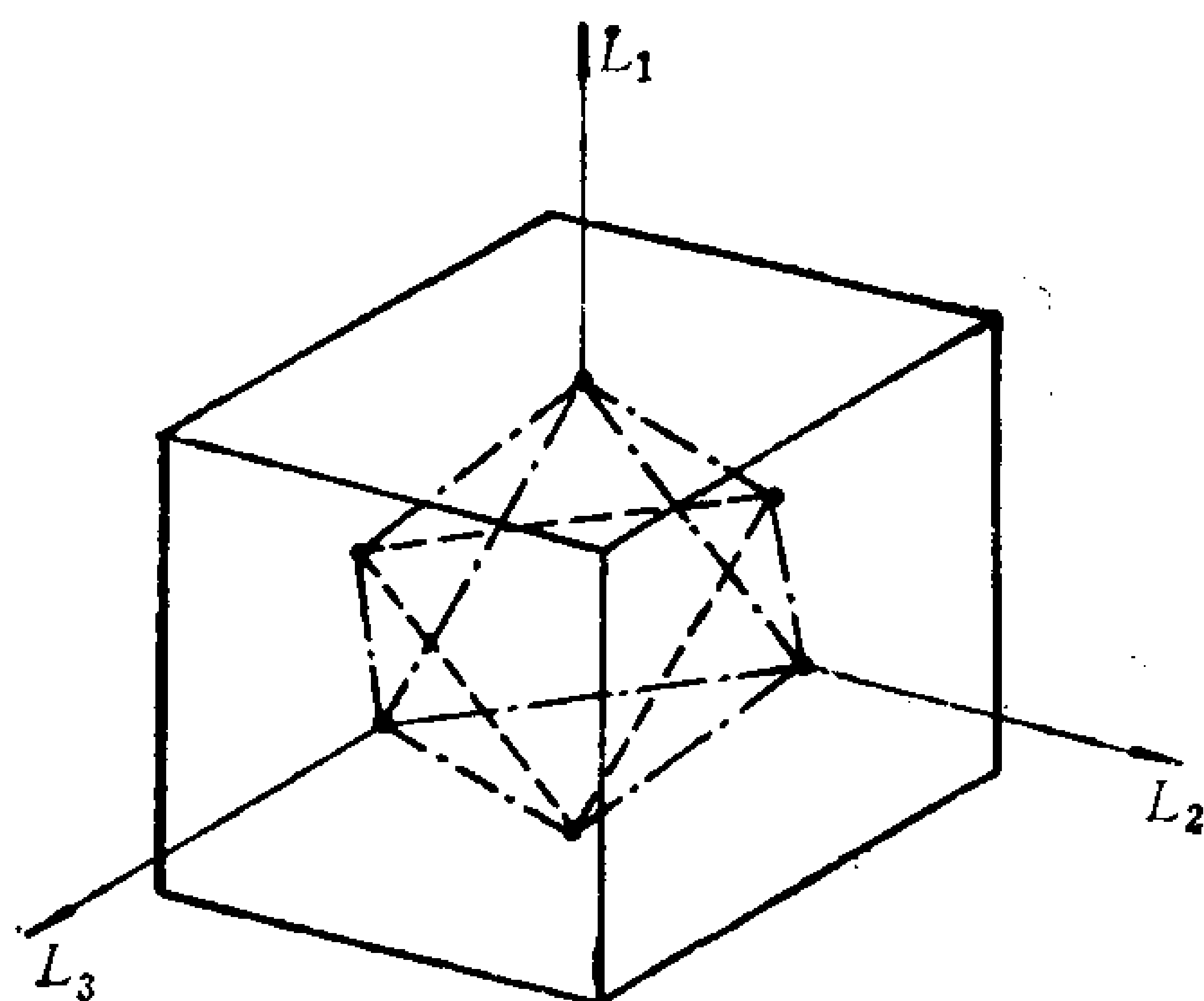


图 4-9

显然，群G是这正八面体的完全旋转对称群O（参见§4.4)的子群。已知$|O|=24$，于是$G=O$。

④ $n_1=2$，$n_2=3$，$n_3=5$，$|G|=60$。

解④可知群G有6个5阶轴，10个3阶轴，15个2阶轴。在6个5阶轴L_1，$L_2,\cdots,L_6$上的12个极点构成一个轨道。群G在这轨道上的作用是非平凡的和可迁的。下边用处理②，③类似的方法来讨论④。选定轴L_1，它以$\boldsymbol{x}_1$和$\boldsymbol{x}_2$为极点。固定$\boldsymbol{x}_1$和$\boldsymbol{x}_2$的转动子群是循环群C_5，C_5的生成元为$g=C_{L_1}\left(\frac{2\pi}{5}\right)$。对上边提到的12个极点适当编号，使得$g$对这轨道的作用可用下面的置换表示：

$$(\boldsymbol{x}_1)(\boldsymbol{x}_2)(\boldsymbol{x}_3\ \boldsymbol{x}_4\ \boldsymbol{x}_5\ \boldsymbol{x}_6\ \boldsymbol{x}_7)(\boldsymbol{x}_8\ \boldsymbol{x}_9\ \boldsymbol{x}_{10}\ \boldsymbol{x}_{11}\ \boldsymbol{x}_{12})。$$

这表明，子群C_5将这轨道分成4个轨道：

$$\{\boldsymbol{x}_1\}，\{\boldsymbol{x}_2\}，\{\boldsymbol{x}_3,\boldsymbol{x}_4,\boldsymbol{x}_5,\boldsymbol{x}_6,\boldsymbol{x}_7\}，\{\boldsymbol{x}_8,\boldsymbol{x}_9,\boldsymbol{x}_{10},\boldsymbol{x}_{11},\boldsymbol{x}_{12}\}。$$

把$\boldsymbol{x}_1$和$\boldsymbol{x}_2$取作球面B的北极和南极，那末其余10个极点不可能全在赤道上。假定$\boldsymbol{x}_3$位于北半球，于是$\boldsymbol{x}_4$，…，$\boldsymbol{x}_7$这5个极点都位于北半球，而且$\|\boldsymbol{x}_1-\boldsymbol{x}_i\|=\|\boldsymbol{x}_1-\boldsymbol{x}_j\|$，$3\leqslant i,j\leqslant 7$，$i\neq j$。其余的5个极点在南半球，因为极点是以形式$\boldsymbol{x}$，$-\boldsymbol{x}$成对出现的，而且$\|\boldsymbol{x}_2-\boldsymbol{x}_i\|=\|\boldsymbol{x}_2-\boldsymbol{x}_j\|$，$8\leqslant i,j\leqslant 12$，$i\neq j$。

由于对轴 L_1 的选择是任意的，可得：每个极点都有 5 个与它距离相等的近的极点，有 5 个远的极点和 1 个在同一轴上的相对极点。把每一点与它近的且与它距离相等的 5 个极点用直线联结起来，得到一个正二十面体，参见图4-6。已知正二十面体的旋轴对称群 I，G 显然是 I 的子群，再由 $|G|=|I|=60$，得到 $G=I$。

到此为止，已找到了所有的第一类点群，它们是：循环群 C_m，二面体群 $D_m(m\geqslant 2)$，正四面体的旋转对称群 T，正八面体的旋转对称群 O 和正二十面体的旋转对称群 I。显然，这些群是彼此不同构的。

§ 4.6　第二类点群

从定理4.3.3和上一节的结果，已能从第一类点群得到全部第二类点群。首先，列出由一个第一类点群 K 和反演 I 生成的群 G。确切地说，$G=\langle K, I\rangle=K\cup IK\cong K\times H$，其中子群 $H=\{E, I\}$，$|G|=2|K|$。

（1）$C_n\cup IC_n\cong C_n\times C_2$。

这里，C_n 是由绕某个轴 l 转动 $\frac{2\pi}{n}$ 的旋转 $C_l\left(\frac{2\pi}{n}\right)$ 生成的 n 阶循环群，C_2 是由反演 I 生成的 2 阶循环群。这是一个交换群，有 $2n$ 个共轭类，每一类只有一个元素。当 n 是奇数时，有 $C_n\times C_2\cong C_{2n}$。然而这两个群不是 $E(3)$ 的共轭子群。此外，$D_2\cong C_2\cup IC_2$。

（2）$D_n\cup ID_n$，$n\geqslant 2$。

这是一个 $4n$ 阶群。已知，当 n 为奇数时，有 $n+3$ 个共轭类；当 n 为偶数时，有 $n+6$ 个共轭类；当 $n\geqslant 3$，且为奇数时，有同构关系 $D_n\cup ID_n\cong D_{2n}$。

（3）$T\cup IT=T_h$。

从 § 4.4知道，T_h 是24阶群，共有 8 个共轭类。

（4）$O\cup IO=O_h$。

从 § 4.4知道，群 O_h 是正八面体的完全对称群，是 48 阶群，

共有12个共轭类。

（5）$Y\cup IY=Y_h$。

从§4.4知道，群 Y_h 是正二十面体的完全对称群，是120阶群，共有10个共轭类。

下边，根据定理4.3.3的（3），找出其余的第二类点群。这就是要找包含有一个指数为2的子群K的第一类点群G^+，从$G^+=K\cup K^+$就可以得到同构于（但不共轭于）G^+的第二类点群$G=K\cup IK^+$。由于$G^+\cong G$，G的乘法表和共轭类的数目和G^+是一样的。然而，G和G^+作为变换群来说是不一样的。G含有转动反演I，G^+则不含有I。

（6）$G^+=C_{2n}$，$K=C_n$，$G=K\cup IK^+$，$|G|=2n$。

（7）$G^+=D_n$，$K=C_n$，$G=K\cup IK^+$，$|G|=2n$，$n\geqslant 2$。

（8）$G^+=D_{2n}$，$K=D_n$，$G=K\cup IK^+$，$|G|=4n$，$n\geqslant 2$。

（9）$G^+=I_d$，$K=T$，$G=K\cup IK^+$，$|G|=24$。

以上各式中，K^+均由定理4.3.3的（3）给出，K^+是由G^+和K决定。

在一般涉及应用点群的物理或化学的书中，都采用熊夫里（Schöenfies）的分类方法和记号。型（9）的群，在熊夫里记号中，通常记为I_d。T是T_d的正规子群，T_d是正四面体的完全对称群。（7）型的群记作C_{nv}，$n=2, 3, \cdots$。群C_{nv}为n角锥体的完全对称群，它包含由垂直于角锥体底面的n阶轴的转动所生成的转动子群C_n，以及通过这个轴的n个垂直平面的反射。

对（1），（2），（6），（8）型群，熊夫里是采用另一种方法来分类的。先看$S_k(\theta)^n$与$C_k(\theta)^n$之间的关系。下面为书写简单起见，将表示转轴的向量$\boldsymbol{k}$省略。计算$S(\theta)^2$：

$$S(\theta)^2=\sigma C(\theta)\sigma C(\theta)=C(\theta)^2,$$

这里，用到性质$\sigma_h C_k(\theta)\sigma_h=C_{-\sigma_h(k)}(\theta)$和$-\sigma_k(\boldsymbol{k})=\boldsymbol{k}$。于是

$$S(\theta)^{2m}=C(\theta)^{2m}。$$

当n为奇数时，$S\left(\frac{2\pi}{n}\right)^n=S\left(\frac{2\pi}{n}\right)^{n-1}S\left(\frac{2\pi}{n}\right)=C\left(\frac{2\pi}{n}\right)^{n-1}$

$\cdot\sigma C\left(\frac{2\pi}{n}\right)=\sigma$，$S\left(\frac{2\pi}{n}\right)^{2n}=E$。当 n 为偶数时，$S\left(\frac{2\pi}{n}\right)^{n}=C\left(\frac{2\pi}{n}\right)^{n}=E$。因此，将 n 为奇数的(1)型群 $C_n\cup IC_n$ 和 n 为偶数的(6)型群合并在一起，给出由 $S\left(\frac{\pi}{n}\right)$ 生成的 $2n$ 阶循环群，用 S_{2n} 表示。$S\left(\frac{\pi}{n}\right)$ 的偶次幂生成子群 C_n。把 n 为偶数的(1)型群和 n 为奇数的(6)型群合并在一起，给出交换群 C_{nh}，它由 $C\left(\frac{2\pi}{n}\right)$ 和 $S\left(\frac{2\pi}{n}\right)$ 生成，即由 $2n$ 个绕固定轴的转角为 $\frac{2\pi}{n}$ 的倍数的转动和转动反演所组成。把 n 为偶数的(2)型群和 n 为奇数的(8)型群合并在一起，给出阶为 $4n$ 的群 D_{nh}，它是 n 棱柱体的完全对称群，C_{nh} 是它的 $2n$ 阶子群。把 n 为奇数的(2)型群和 n 为偶数的(8)型群合并在一起，给出阶为 $4n$ 的群 D_{nd} 群，它为扭转 n 棱柱体的完全对称群，S_{2n} 是它的 $2n$ 阶子群。以上的结果即：

$$S_{2n}=\begin{cases}C_n\cup IC_n, & n\text{ 是奇数},\\ C_{2n}, & n\text{ 是偶数};\end{cases}$$

$$C_{nh}=\begin{cases}C_n\cup IC_n, & n\text{ 是偶数},\\ C_{2n}, & n\text{ 是奇数};\end{cases}$$

$$D_{nh}=\begin{cases}D_n\cup ID_n, & n\text{ 是偶数},\\ D_{2n}, & n\text{ 是奇数};\end{cases}$$

$$D_{nd}=\begin{cases}D_n\cup ID_n, & n\text{ 是奇数},\\ D_{2n}, & n\text{ 是偶数}。\end{cases}$$

§4.7 晶体点群

在这节，将把有限点群的结果用于晶体点群，为此，先介绍有关格群的定义和性质。

定义4.7.1 三维空间平移群$T(3)$的非平凡的离散子群称为格群。

由于$T(3)$的元素T_a完全由向量$\boldsymbol{a}$决定，以及$T_a \cdot T_b = T_{b+a}$，于是可将$T(3)$和它的任何子群看作向量群。向量群的元素是向量，运算是向量加法。显然，向量群是交换群。如果向量群G包含3个线性无关的向量，则它为三维的；如果G只包含2个线性无关向量，称为二维的；如果所有向量是位于经过原点的一条直线上，称它为一维的。

设G是三维格群，$\boldsymbol{a}_1$，$\boldsymbol{a}_2$，$\boldsymbol{a}_3$是包含在G中的三个线性无关向量，那么集合

$$\{m_1\boldsymbol{a}_1 + m_2\boldsymbol{a}_2 + m_3\boldsymbol{a}_3 | m_i \text{ 是整数}, \quad i=1, 2, 3\}$$

是G的子群。将证明，在群G中可适当地选取$\boldsymbol{a}_i$，使得上边集合就是G本身。

定理4.7.1 设G是三维格群，则在G中存在3个线性无关的向量$\boldsymbol{b}_1$，$\boldsymbol{b}_2$，$\boldsymbol{b}_3$，使得每一个$\boldsymbol{a} \in G$能够唯一地表成

$$\boldsymbol{a} = n_1\boldsymbol{b}_1 + n_2\boldsymbol{b}_2 + n_3\boldsymbol{b}_3 \tag{4-10}$$

其中n_i均为整数。

证明 设$\boldsymbol{a}_1$，$\boldsymbol{a}_2$，$\boldsymbol{a}_3$是G中的3个线性无关向量。令P是由这三个向量张成的平行六面体（不只包括内部，而且包括面、棱、顶点）。由于G是离散群，以及原点的G-轨道就是G。因此，G在P中只有有限个元素。设$\boldsymbol{b}_1$是$G \cap P$中平行于$\boldsymbol{a}_1$的最小非零向量。设$\boldsymbol{b}_2 \in G$，它位于$\boldsymbol{a}_1$和$\boldsymbol{a}_2$生成的平行四边形中，而且由$\boldsymbol{b}_1$和$\boldsymbol{b}_2$生成的平行四边形具有最小面积。最后选择$\boldsymbol{b}_3 \in G \cap P$，而且使$\boldsymbol{b}_1$，$\boldsymbol{b}_2$，$\boldsymbol{b}_3$生成的平行六面体$Q$的体积$V(Q)$最小。将证明，按上述方法选取的$\boldsymbol{b}_1$，$\boldsymbol{b}_2$，$\boldsymbol{b}_3$具有式(4-10)的性质。

首先，$\boldsymbol{b}_1$，$\boldsymbol{b}_2$，$\boldsymbol{b}_3$按其选取方式显然是线性无关的。对于任意$\boldsymbol{a} \in G$，有唯一的一组实数α_i，使得

$$\boldsymbol{a} = \alpha_1\boldsymbol{b}_1 + \alpha_2\boldsymbol{b}_2 + \alpha_3\boldsymbol{b}_3.$$

考虑

$$a-\sum_{i=1}^{3}[\alpha_i]b_i=\sum_{i=1}^{3}\beta_i b_i=b$$

其中$[\alpha_i]$表示实数α_i的最大整数部分，$\beta_i=\alpha_i-[\alpha_i]$，$0\leqslant\beta_i<1$。只要能证明$\beta_i=0$，$i=1, 2, 3$，便可得到定理。

若$0<\beta_3<1$，那么由b_1，b_2和$b=\sum_{i=1}^{3}\beta_i b_i$生成的平行六面体$Q'$的体积$V(Q')$比$V(Q)$小，确切地说，$V(Q')=\beta_3 V(Q)$。这可直接由下面的计算得到：

$$\begin{aligned}V(Q')&=b_1\cdot(b_2\times b)=b_1\cdot\left(b_2\times\sum_{i=1}^{3}\beta_i b_i\right)\\&=b_1\cdot(b_2\times\beta_1 b_1+b_2\times\beta_3 b_3)\\&=\beta_3 b_1\cdot(b_2\times b_3)=\beta_3 V(Q),\end{aligned}$$

在这里，"×"是熟知的向量积，"·"是内积。由此结果，得到$V(Q')<V(Q)$。根据对向量b_3选取的要求，必有$b\notin P$。对此，可找到整数m_1和m_2，使得

$$b'=b+m_1 b_1+m_2 b_2\in P。$$

将b和b_i用a_i表出，设

$$b_1=\gamma_{11}a_1$$
$$b_2=\gamma_{21}a_1+\gamma_{22}a_2$$
$$b_3=\gamma_{31}a_1+\gamma_{32}a_2+\gamma_{33}a_3$$
$$b=(\beta_1\gamma_{11}+\beta_2\gamma_{21}+\beta_3\gamma_{31})a_1+(\beta_2\gamma_{22}+\beta_3\gamma_{32})a_2+\beta_3\gamma_{33}a_3,$$

其中$0<\gamma_{ij}\leqslant 1$。令$\delta_1=\beta_1\gamma_{11}+\beta_2\gamma_{21}+\beta_3\gamma_{31}$，$\delta_2=\beta_2\gamma_{22}+\beta_3\gamma_{32}$，和$b'=b-[\delta_1]b_1-[\alpha_2]b_2$。那么

$$b'=(\delta_1-[\delta_1])a_1+(\delta_2-[\delta_2])a_2+\beta_3\gamma_{33}a_3。$$

于是，取$m_1=-[\delta_1]$，$m_2=-[\delta_2]$，则有

$$b'=b+m_1 b_1+m_2 b_2\in P。$$

由b_1，b_2和b'生成的平行六面体Q''的体积$V(Q'')$。

$$\begin{aligned}V(Q'')&=b_1\cdot(b_2\times b')\\&=\beta_3 V(Q)<V(Q)。\end{aligned}$$

这结果与β_3的选取相矛盾，因此只可能$\beta=0$。作与上面类似的讨论，可以得到$\beta_2=\beta_1=0$。于是定理得证。

这个定理告诉我们，格群是有几何意义的，格群的元素可以看作通常意义下的格子点。确切地说，对于任意给定的一点$\boldsymbol{x}\in R^3$，三维格群G作用于$\boldsymbol{x}$得到的G轨道，形成R^3的一组几何格子，简称为**格子**。所有格子的全体，即所有的G轨道，称为**晶格**或**空间格子**。现已能够构造包含任意点$\boldsymbol{x}$的格子，而两点位于同一格子上的充要条件是它们位于同一G轨道中。

设H是一个三维格群，L是H作用于给定点$\boldsymbol{x}$而形成的格子，即$L=H\boldsymbol{x}$。将L的完全对称群记为G。易见，H是G的一个平移子群。将看到，G是离散群，而且$H=G\cap T(3)$。为方便起见，即$\boldsymbol{x}$为原点$\boldsymbol{\theta}$。对于任一变换$T\in G\cap T(3)$，若$T\boldsymbol{\theta}=\boldsymbol{b}$，则$T=T_b$。由于$T\in G$，$T$将$L$映为自身，于是$\boldsymbol{b}$是格子$L$上的一个格点和存在变换$T'\in H$，使得$\boldsymbol{b}=T'\boldsymbol{\theta}$。由于$T$和$T'$都是由$\boldsymbol{b}$决定的平移，必有$T'=T$，于是$T\in H$，$H=G\cap T(3)$。

进一步考虑G与H的关系。对于$g\in G$，和$g\boldsymbol{\theta}=\boldsymbol{b}$，有$\boldsymbol{b}\in L$。由于$H$在格子$L$上是可迁的，则存在$T\in H$，使得$T\boldsymbol{\theta}=\boldsymbol{b}$。于是$T^{-1}g(\boldsymbol{\theta})=\boldsymbol{\theta}$，即$T^{-1}g$是使原点$\boldsymbol{\theta}$不变的变换，$T^{-1}g\in O(3)$。设$T^{-1}g=f$，$g=Tf$。若用$F$表示$G$中所有使原点$\boldsymbol{\theta}$不变的变换组成的群，那么不难验证

$$G=H\rtimes F,$$

即G是群H和F的半直积。G中两元素的积有关系式：

$$(T_1f_1)\cdot(T_2f_2)=T_1f_1T_2f_1^{-1}\cdot f_1f_2,$$

和

$$f_1Tf_1^{-1}\in T(3)\cap G=H。$$

由于以原点为中心的任意球B_r内都只有有限个格点，和G的元素是保距的，因此F是有限点群，进而G是离散群。又任何两个三维格群显然是同构的。根据$G=H\rtimes F$，如果不计同构，要决定格子的所有完全对称群，只要计算出所有可能的点群F就可以

了。L 的任意对称群 G'（不必是完全对称群），是指 G 的一个任意子群。

定义4.7.2 令点 $\boldsymbol{x}\in R^3$。把包含点 $\boldsymbol{x}$ 的三维格子 L 映为它自身而且使点 $\boldsymbol{x}$ 不变的 $E(3)$ 的子群，称为**晶体点群**。$\boldsymbol{x}$ 点处的最大晶体点群 F，称为 L 在 $\boldsymbol{x}$ 的**全面对称**。

已证明，晶体点群必定是有限点解。然而，其逆并不成立，即并不是所有的有限点群都是晶体点群。点群的元素要求使格子 L 不变，这是一个很强的限制。

定理4.7.2 设 K 是晶体点群。若 $g\in K$ 是一个非平凡(即非恒等）转动，则 g 的阶只可能是2，3，4，6。若 $g=Ik$，是 K 中的转动反演，其中 k 是转动，则转动 k 的阶只可能是1，2，3，4，6。

证明：若点 $\boldsymbol{x}$ 和 $\boldsymbol{y}$ 含于同一格子 L 内，那么，不难证明，分别使点 $\boldsymbol{x}$ 和 $\boldsymbol{y}$ 不动的全面对称在 $E(3)$ 中是共轭子群（请读者将此证明补出）。据此，为了证明定理4.7.2，只需对于点 $\boldsymbol{x}$ 为原点证明就够了。设 H 是三维空间群，格子 $L=H\boldsymbol{\theta}$，H 的基本向量是 $\boldsymbol{b}_1$，$\boldsymbol{b}_2$，$\boldsymbol{b}_3$。对于非平凡转动 $g\in K$，考虑它在基底 $\boldsymbol{b}_i$ 之下的矩阵表示。若 $g\boldsymbol{b}_i=\sum_{j=1}^{3}C_{ji}\boldsymbol{b}_j$，由于 $\boldsymbol{b}_i$ 是 H 的基本向量和 $H\boldsymbol{\theta}=H$，那么 C_{ji} 必定是整数，矩阵 $C=(C_{ij})$ 的迹 $\mathrm{tr}\,C=\sum_{i=1}^{3}C_{ii}$ 当然也是整数。另一方面，转动 g 在一组适当的基底之下可有矩阵表示 C'

$$C'=\begin{pmatrix}\cos\theta & -\sin\theta & 0\\ \sin\theta & \cos\theta & 0\\ 0 & 0 & 1\end{pmatrix},$$

$\mathrm{tr}C'=1+2\cos\theta$，其中 θ 是 g 的旋转角度。根据线性代数的基本知识，知道相似矩阵的迹是相同的。因此，$1+2\cos\theta$ 是整数。这

时 θ 只可能是$\frac{\pi}{2}$，$\frac{3}{2}\pi$，$\frac{n}{3}\pi$，$n=0, 1, 2, 3, 4, 5$。g 的阶只可能是2，3，4，6。若 g 是转动反演，g 的迹是 $-(1+2\cos\theta)$，相应的转动 k 的阶只可能是1，2，3，4，6。

这个定理证明了晶体点群不可能有5阶和大于6阶的元素。所以从前面点群分类的讨论中可知，只有下列32个点群才可能是晶体点群：在第一类点群中有循环群 C_1，C_2，C_3，C_4，C_6，二面体群 D_2，D_3，D_4，D_6，四面体群 T 和八面体群 O；在第二类点群中有 S_2，S_4，S_6，C_{1h}，C_{2h}，C_{3h}，C_{4h}，C_{6h}，C_{2v}，C_{3v}，C_{4v}，C_{6v}，D_{2h}，D_{3h}，D_{4h}，D_{6h}，D_{2d}，D_{3d}，T_h，T_d，O_h。事实上，可以证明，这32个点群确是某些格子的对称群，结晶学上把它们称为32个晶类。

晶体点群共有32个，从上面的讨论可知，这是一个不太复杂的结果，但是很有意义。因为从这32个晶体点群出发，可以找出230个结晶群。找出这230个结晶群并证明此外没有其它的结晶群，这一工作是群论对其它自然科学的首次成功的重大应用，同时它也推动了群论本身的发展。

第五章　典　型　群

实数域和复数域上的典型群在上个世纪就出现在几何学和物理学中，进而在十九世纪末发现它们在复单李群和实单李群分类中的突出地位，使得它们在数学中一直受到重视与研究。现在对于一般域上典型群的研究已经作的比较彻底，人们的注意力已经转到更一般的环上的典型群的研究。

在这一章主要介绍域上典型群的结构，包括域上的一般线性群、特殊线性群、辛群和正交群。对于定理的证明，则采取矩阵方法和几何方法同时并用的原则。希望读者一方面学习矩阵运算的技巧，一方面学习问题的几何处理。

§5.1　线性群的结构

域F上n维线性空间V的所有可逆线性变换对于通常的线性变换乘法成群，记作$GL_n(V)$，称为域F上的n级**一般线性群**。利用线性变换和它在V的给定基底之下的矩阵表示之间的一一对应，得到$n\times n$可逆矩阵全体对于通常的矩阵乘法成群，用$GL_n(F)$表示此群，有$GL_n(F)$与$GL_n(V)$同构。在这节，主要用矩阵工具讨论线性群结构，其目的是希望读者从中学习一些矩阵运算的技巧。

用F^*表示域F的非零元全体组成的乘法群。考虑$GL_n(F)$到F^*的同态映射$\det: GL_n(F)\to F^*$，它把F上$n\times n$可逆阵A映到A的行列式$\det A$，同态det的核是行列式为1的矩阵全体，用$SL_n(F)$表示。通常称$SL_n(F)$为域F上的n级**特殊线性群**。显然，$SL_n(F)$是$GL_n(F)$的正规子群，而且有$GL_n(F)/SL_n(F)\cong F^*$。

定理5.1.1　域F上的n级特殊线性群$SL_n(F)$是由初等矩阵$T_{ij}(b)=I+be_{ij}$生成的群，其中$i\neq j$，$1\leqslant i, j\leqslant n$，

$b\in F$，I 是单位阵，e_{ij} 是在（i，j）位置为1在其余位置全为0的 $n\times n$ 阵，即

$$SL_n(F)=\langle T_{ij}(b)\mid i\neq j,\ 1\leqslant i,j\leqslant n,\ b\in F\rangle。$$

这个定理的证明，作为一个练习留给读者。

下面给出两个等式，它们在后面的讨论中是很有用的。

$$\begin{pmatrix}0&1\\-1&0\end{pmatrix}=\begin{pmatrix}1&0\\-1&1\end{pmatrix}\begin{pmatrix}1&1\\0&1\end{pmatrix}\begin{pmatrix}1&0\\-1&1\end{pmatrix}\qquad(5\text{-}1)$$

$$\begin{pmatrix}\lambda&0\\0&\lambda^{-1}\end{pmatrix}=\begin{pmatrix}1&-\lambda\\0&1\end{pmatrix}\begin{pmatrix}1&0\\\lambda^{-1}&1\end{pmatrix}\begin{pmatrix}0&1\\-1&0\end{pmatrix}\begin{pmatrix}1&0\\\lambda&1\end{pmatrix}\qquad(5\text{-}2)$$

其中 $\lambda\in F^*$。

由式（5-1），有

$$\begin{pmatrix}0&1&&&&\\-1&0&&&&\\&&1&&&\\&&&1&&\\&&&&\ddots&\\&&&&&1\end{pmatrix}\in SL_n(F),$$

由式（5-2）有

$$\begin{pmatrix}\lambda&&&&&\\&\lambda^{-1}&&&&\\&&1&&&\\&&&1&&\\&&&&\ddots&\\&&&&&1\end{pmatrix}\in SL_n(F)。$$

系5.1.1 $GF_n(F)$ 中每一个元皆可表成

$$B\begin{pmatrix}1&&&&\\&1&&&\\&&\ddots&&\\&&&1&\\&&&&\lambda\end{pmatrix}=BD(\lambda),$$

其中$B\in SL_n(F)$，$\lambda\in F^*$，$D(\lambda)=\begin{pmatrix}1&&&&\\&1&&&\\&&\ddots&&\\&&&1&\\&&&&\lambda\end{pmatrix}$。

证明 对于$A\in GL_n(F)$，若$\det A=\lambda\in F^*$，则

$$A\begin{pmatrix}1&&&&\\&1&&&\\&&\ddots&&\\&&&1&\\&&&&\lambda^{-1}\end{pmatrix}=B\in SL_n(F)。$$

于是

$$A=B\begin{pmatrix}1&&&&\\&1&&&\\&&\ddots&&\\&&&1&\\&&&&\lambda\end{pmatrix}。$$

定理5.1.2 令F是域，$n>1$，则

（1）除了$n=2$和$|F|=2$或3（这里$|F|$表示域F的元素个数）这两种情形外，$SL_n(F)$是$GL_n(F)$的换位子群，也是它自己的换位子群，即

$$SL_n(F)=[SL_n(F),\ SL_n(F)]=[GL_n(F),\ GL_n(F)]。$$

（2）$SL_n(F)$的中心$C(SL_n(F))=F^*I\cap SL_n(F)$，$GL_n(F)$的中心$C(GL_n(F))=F^*I$。

证明 （1）为了证明$SL_n(F)=[SL_n(F),\ SL_n(F)]$，只要证明$SL_n(F)$的每一个生成元$T_{ij}(b)\in[SL_n(F),SL_n(F)]$就够了。如果$n\geqslant 3$，选取$k\neq j$，$i$，则

$$T_{ij}(b)=[T_{ik}(b),\ T_{kj}(1)]。$$

如果$n=2$，则有$\begin{pmatrix}d&\\&d^{-1}\end{pmatrix}$和$\begin{pmatrix}1&c\\0&1\end{pmatrix}$的换位子

$$\left[\begin{pmatrix}d&\\&d^{-1}\end{pmatrix},\ \begin{pmatrix}1&c\\0&1\end{pmatrix}\right]=\begin{pmatrix}1&c(d^2-1)\\0&1\end{pmatrix},$$

若$|F|\geqslant 4$，那么可以选取$d\neq 0$和$d\neq\pm 1$，对于任意给定的元素$b\in F$，令$c=(d^2-1)^{-1}b$，则

$$T_{12}(b)=\left[\begin{pmatrix} d & \\ & d^{-1}\end{pmatrix},\ \begin{pmatrix} 1 & c \\ 0 & 1\end{pmatrix}\right]\in[SL_n(F),\ SL_n(F)]。$$

同样可以证明$T_{21}(b)\in[SL_n(F),\ SL_n(F)]$。于是得到

$$SL_n(F)=[SL_n(F),\ SL_n(F)] \tag{5-3}$$

进而，由于$GL_n(F)/SL_n(F)\cong F^*$和F^*是交换群，则有$SL_n(F)\supset[GL_n(F),\ GL_n(F)]$。另一方向的包含关系，由于已有式(5-3)，是显然的。于是得到

$$SL_n(F)=[GL_n(F),\ GL_n(F)]。$$

(2) 请读者证明。

通常称因子群$SL_n(F)/C(SL_n(F))$为**射影特殊线性群**，用$PSL_n(F)$表示。这节下面的主要内容是要证明，除了某些特殊情形外，$PSL_n(F)$是单群。

到目前为止，$SL_n(F)$已有三种不同的刻化方式：

(a) $SL_n(F)=\langle T_{ij}(b)\in GL_n(F)\mid i\neq j,\ b\in F\rangle$。

(b) $SL_n(F)=\{A\in GL_n(F)\mid\det A=1\}$。

(c) $SL_n(F)=[GL_n(F),\ GL_n(F)]$，(除$n=2$，$|F|=2,\ 3$)。

进而，希望几何地刻化出$SL_n(F)$。

设V是域F上的n维线性空间。线性变换$\sigma\in GL(V)$，$1=1_V$是V上的恒等变换。线性变换$\sigma-1$的像空间$\mathrm{Im}(\sigma-1)=(\sigma-1)V$。根据线性代数的知识，有$\dim\mathrm{Im}(\sigma-1)=\dim((\sigma-1)V)=\mathrm{rank}(\sigma-1)$，其中$\mathrm{rank}(\sigma-1)$表示线性变换$\sigma-1$的秩。通常称$\mathrm{rank}(\sigma-1)$为$\sigma$的**剩余数**，用$\mathrm{res}\sigma$表示。$GL(V)$中剩余数是1的元素是最使人们感兴趣的。例如，$T_{ij}(b)(b\neq 0)$的剩余数就是1。

令$R=\mathrm{Im}(\sigma-1)=(\sigma-1)V$，$P=\mathrm{Ker}(\sigma-1)$。设$\sigma$的剩余数是1，即$\mathrm{rank}(\sigma-1)=1$，则$V$的子空间$R$和$P$的

维数分别是$\dim R=1$和$\dim P=n-1$。下面分二种情形讨论：

（1）$P\supsetneq R$。

这时，有$V=P\oplus R$，即V是子空间P和R的直和。设$P=F\boldsymbol{v}_1\oplus\cdots\oplus F\boldsymbol{v}_{n-1}$，$R=F\boldsymbol{v}_n$，那么相对$V$的基底（$\boldsymbol{v}_1$，$\boldsymbol{v}_2$，…，$\boldsymbol{v}_n$），由于$(\sigma-1)\boldsymbol{v}_i=\boldsymbol{0}$，$i=1,2,\cdots,n-1$，$(\sigma-1)\boldsymbol{v}_n=\lambda\boldsymbol{v}_n$，$\lambda\neq 0$，于是线性变换$\sigma-1$的阵表示是

$$\begin{pmatrix} 0 & & & \\ & 0 & & \\ & & \ddots & \\ & & & 0 & \\ & & & & \lambda \end{pmatrix}\qquad \lambda\in F^*,$$

σ的阵表示是

$$\begin{pmatrix} 1 & & & & \\ & 1 & & & \\ & & \ddots & & \\ & & & 1 & \\ & & & & 1+\lambda \end{pmatrix}=D(1+\lambda)。$$

由此阵表示，得到$\sigma\boldsymbol{v}_i=\boldsymbol{v}_i$，$i=1,2,\cdots,n-1$，$\sigma\boldsymbol{v}_n=(1+\lambda)\boldsymbol{v}_n$。

（2）$P\supseteq R$。

取$\boldsymbol{v}_n\in V\setminus P$，则$V=P\oplus F\boldsymbol{v}_n$。设子空间$P$的基底为（$\boldsymbol{v}_1$，…，$\boldsymbol{v}_{n-1}$），则（$\boldsymbol{v}_1$，…，$\boldsymbol{v}_{n-1}$，$\boldsymbol{v}_n$）构成$V$的基底。设$R=F\boldsymbol{a}\subseteq P$，则$(\sigma-1)\boldsymbol{v}_i=0$，$i=1,2,\cdots,n-1$，$(\sigma-1)\boldsymbol{v}_n=\lambda\boldsymbol{a}$，其中$\lambda\in F^*$。于是对任一元$\boldsymbol{x}=\sum\limits_{i=1}^{n}c_i\boldsymbol{v}_i\in V$，有$(\sigma-1)\boldsymbol{x}=\lambda c_n\boldsymbol{a}$，即$\sigma\left(\sum\limits_{i=1}^{n}c_i\boldsymbol{v}_i\right)=\sum\limits_{i=1}^{n}c_i\boldsymbol{v}_i+\lambda c_n\boldsymbol{a}$。由此得到一个由$V$到$F$的线性函数$\rho$，$\rho$：$V\to F$，它由$\rho\left(\sum\limits_{i=1}^{n}c_i\boldsymbol{v}_i\right)=\lambda c_n$给出。设$\boldsymbol{a}=\sum\limits_{i=1}^{n-1}b_i\boldsymbol{v}_i$，则$(\sigma-1)\boldsymbol{v}_n=$

$\lambda a = \sum_{i=1}^{n-1} \lambda b_i v_i$，于是$\sigma$在基底（$v_1$，…，$v_n$）下的阵表示为

$$\begin{pmatrix} 1 & & & \lambda b_1 \\ & 1 & & \vdots \\ & & \ddots & \lambda b_{n-1} \\ & & & 1 \end{pmatrix}$$

由于$R = Fa \subseteq P$，根据替换定理，可以选取 $v_1 = a_1$，这时σ有阵表示

$$\begin{pmatrix} 1 & & & & \lambda \\ & 1 & & & 0 \\ & & \ddots & & \vdots \\ & & & 1 & 0 \\ & & & & 1 \end{pmatrix} = T_{1n}(\lambda),\quad \lambda \in F^*。$$

由以上讨论，可得如下定理。

定理5.1.3 设V是域F上n维线性空间，$\sigma \in GL(V)$，σ的剩余数$\mathrm{res}\,\sigma = 1$。令$P = \mathrm{Ker}(\sigma - 1)$，$R = \mathrm{Im}(\sigma - 1)$。那么

（1）若$R \subsetneq P$，则可在V中选一基底，使得σ的阵表示为对角阵

$$\begin{pmatrix} 1 & & & & \\ & 1 & & & \\ & & \ddots & & \\ & & & 1 & \\ & & & & \mu \end{pmatrix} = [1,\ 1,\ \cdots,\ 1,\ \mu],\ \mu \in F^*。$$

而且μ由σ唯一决定。

（2）若$R \subseteq R$，则可在V中选一基底，使得σ的阵表示为

$$\begin{pmatrix} 1 & & & \lambda \\ & 1 & & \\ & & \ddots & \\ & & & 1 \end{pmatrix} = T_{1n}(\lambda),\quad \lambda \in F^*。$$

（3）$R \subseteq P$，当且仅当存在一线性函数$\rho \in V^*$，它对任何u

$\in P$均有$\rho(\boldsymbol{u})=\mathbf{0}$和向量$\boldsymbol{a}(\neq 0)\in P$使得对任何$\boldsymbol{v}\in V$，

$$\sigma(\boldsymbol{v})=\boldsymbol{v}+\rho(\boldsymbol{v})\boldsymbol{a}。\tag{5-4}$$

对于$\mathrm{rank}(\sigma-1)=1$和$(\sigma-1)V\subsetneq\mathrm{Ker}(\sigma-1)$的$\sigma$称为**$D$变换**，而对于满足$\mathrm{rank}(\sigma-1)=1$和$(\sigma-1)V\subseteq\mathrm{Ker}(\sigma-1)$的$\sigma$称为**平延**。容易看出，$\sigma$为平延当且仅当$\mathrm{res}\,\sigma=1$和$(\sigma-1)^2=0$。

定理5.1.4 设$SL(V)$是由$GL(V)$中所有平延生成的群。对于V的任意给定的基底，将V上线性变换与它在此基底下的阵表示相对应，则此对应是群$SL(V)$和群$SL_n(F)$之间的同构映射。

证明 首先任意给定V的基底$(\boldsymbol{e}_1, \boldsymbol{e}_2, \cdots, \boldsymbol{e}_n)$，并设$f$是$V$上线性变换与它在这基底下的阵表示之间的对应，则已知f给出$GL(V)$和$GL_n(F)$之间的同构。事实上可以证明，f也给出$SL(V)$和$SL_n(F)$之间的同构。为此只要证明$GL(V)$中每一个平延对应的阵在$SL_n(F)$中，即$f(SL(V))\subset SL_n(F)$，和$SL_n(F)$的每个生成元$T_{ij}(\lambda)$决定的线性变换是一个平延就行了。

设平延$\sigma\in SL(V)$在基底$(\boldsymbol{e}_1, \cdots, \boldsymbol{e}_n)$之下的阵表示为$T$。由定理5.1.3的（2），存在$V$的一个基底$(\boldsymbol{v}_1, \cdots, \boldsymbol{v}_n)$，$\sigma$在此基底下的阵表示为$T_{1n}(\lambda)$。令$P_1$是将基底$(\boldsymbol{e}_1, \cdots, \boldsymbol{e}_n)$映到$(\boldsymbol{v}_1, \cdots, \boldsymbol{v}_n)$的线性变换，则

$$T=P_1T_{1n}(\lambda)P_1^{-1},\quad P_1\in GL_n(F)。$$

设$P_1=BD(\mu)$，其中$B\in SL_n(F)$，$\mu\in F^*$，于是

$$T=BT_{1n}(\lambda\mu^{-1})B^{-1}\in SL_n(K)。$$

另一方面，对于$SL_n(F)$的生成元$T_{ij}(\lambda)$，有$\mathrm{rank}(T_{ij}-I)=1$和$(T_{ij}-I)^2=0$。因此，$T_{ij}(\lambda)$作为$V$上的线性变换是平延。于是$f(SL(V))=SL_n(F)$，$SL(V)\cong SL_n(F)$。进而，$T_{ij}(\lambda)$可以表成定理5.1.3中式（5-4）的形式。设$\boldsymbol{v}$在基底$(\boldsymbol{e}_1, \cdots, \boldsymbol{e}_n)$下的坐标表示为$(a_1, a_2, \cdots, a_n)'$，其中“$'$”表示矩阵的转置，则

$$T_{ij}(\lambda)v=T_{ij}(\lambda)\begin{pmatrix}a_1\\a_2\\\vdots\\a_n\end{pmatrix}$$

$$=\begin{pmatrix}a_1\\a_2\\\vdots\\a_n\end{pmatrix}+\lambda\begin{pmatrix}0\\\vdots\\0\\a_j\\0\\\vdots\\0\end{pmatrix}i\text{-行}$$

$$=\begin{pmatrix}a_1\\a_2\\\vdots\\a_n\end{pmatrix}+\begin{pmatrix}0\\0\\\vdots\\0\\1\\0\\\vdots\\0\end{pmatrix}(\underset{i\text{-行}}{0},\ \cdots,\quad 0,\ \underset{j\text{-列}}{\lambda},\ 0\cdots0)\begin{pmatrix}a_1\\a_2\\\vdots\\a_n\end{pmatrix}$$

$$=v+a\rho(v)=v+\rho(v)a,$$

其中 $a=\begin{pmatrix}0\\\vdots\\0\\1\\0\\\vdots\\0\end{pmatrix}i$ 行，$\rho(v)=\lambda a_j$。

这个定理说明 $SL_n(F)$ 是由平延生成的群。

下面讨论群 $SL_n(F)$ 的单性，从而可以看到平延在其中起着重要作用。

引理5.1.1 设 $\mathfrak{N}$ 是 $GL_n(F)$ 的子群，而且它在群 $SL_n(F)$ 下不变，即对于任何 $A\in SL_n(F)$，都有 $A\mathfrak{N}A^{-1}\subseteq\mathfrak{N}$。那么，如

果$\mathfrak{N}$包有一个平延，则$\mathfrak{N}\supseteq SL_n(F)$。

证明 设T是平延而且$T\in\mathfrak{N}$。在n维线性空间V中选一组适当的基底，使得T有阵表示$T_{1n}(\lambda)$，于是T与$T_{1n}(\lambda)$在$GL_n(F)$下共轭（即存在$P\in GL_n(F)$，使得$T=PT_{1n}(\lambda)P^{-1}$），用$T\sim T_{1n}(\lambda)$表示。分二种情形讨论：

（1）$n\geqslant 3$。将证明任何两个平延在$SL_n(F)$中共轭。由此，再考虑到$SL_n(F)$由平延生成，便得到引理。

从前边的讨论已得到$T\sim T_{1n}(\lambda\mu^{-1})$，即存在$P\in SL_n(F)$，使$T=PT_{1n}(\lambda\mu^{-1})P^{-1}$。因此要证明任何两个平延共轭，只要证明$T_{1n}(\lambda\mu^{-1})$与$T_{1n}(1)$在$SL_n(F)$中共轭就够了。而这个结论可由下面的简单计算得出：

$$\begin{pmatrix}\lambda & & \\ & \lambda^{-1}\mu^{-1} & \\ & & \mu\end{pmatrix}\begin{pmatrix}1 & & 1\\ & 1 & \\ & & 1\end{pmatrix}\begin{pmatrix}\lambda & & \\ & \lambda^{-1}\mu^{-1} & \\ & & \mu\end{pmatrix}^{-1}=T_{13}(\lambda\mu^{-1})$$

（2）$n=2$。由于T与$T_{12}(\lambda)$在$SL_2(F)$中共轭，令

$$\mathfrak{N}'=\begin{pmatrix}1 & 0\\ 0 & \lambda\end{pmatrix}\mathfrak{N}\begin{pmatrix}1 & 0\\ 0 & \lambda\end{pmatrix}^{-1},$$ 则$\mathfrak{N}'\ni T_{12}(1)$。容易验证$\mathfrak{N}'$在$SL_2(F)$下不变。因此，要证明$\mathfrak{N}\supseteq SL_2(F)$，只需证明$\mathfrak{N}'\supseteq SL_2(F)$。考虑

$$\begin{pmatrix}\lambda & 0\\ 0 & \lambda^{-1}\end{pmatrix}\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}\begin{pmatrix}\lambda & \\ & \lambda^{-1}\end{pmatrix}^{-1}=\begin{pmatrix}1 & \lambda^2\\ 0 & 1\end{pmatrix}\in\mathfrak{N}'$$

对一切$\lambda\in F^*$，于是$\mathfrak{N}'$包有

$$\begin{pmatrix}1 & (\lambda+1)^2\\ 0 & 1\end{pmatrix}\begin{pmatrix}1 & \lambda^2\\ 0 & 1\end{pmatrix}^{-1}\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}^{-1}=\begin{pmatrix}1 & 2\lambda\\ 0 & 1\end{pmatrix}$$

对一切$\lambda\in F^*$。

如果域F的特征$\neq 2$，则当λ跑遍F^*时，2λ也跑遍F^*。因此$\mathfrak{N}'$包有$T_{12}(\lambda)$，对所有$\lambda\in F^*$。又因为

$$\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix}\begin{pmatrix}1 & -\mu\\ 0 & 1\end{pmatrix}\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix}^{-1}=\begin{pmatrix}1 & 0\\ \mu & 1\end{pmatrix},$$

于是$\mathfrak{N}'$包有$T_{21}(\mu)$，对一切$\mu\in F^*$。因此有$\mathfrak{N}'\supseteq SL_2(F)$。

如果域F的特征$=2$，仍有上面的结果。已经得到$\mathfrak{N}'$包有$T_{12}(1)$和$T_{12}(\lambda^2)$，对一切$\lambda\in F^*$。考虑

$$\begin{pmatrix}0&1\\1&0\end{pmatrix}\begin{pmatrix}1&1\\0&1\end{pmatrix}\begin{pmatrix}0&1\\1&0\end{pmatrix}^{-1}=\begin{pmatrix}1&0\\1&1\end{pmatrix}\in\mathfrak{N}',$$

于是

$$\begin{pmatrix}\lambda^{-1}&0\\0&\lambda\end{pmatrix}\begin{pmatrix}1&0\\1&1\end{pmatrix}\begin{pmatrix}\lambda^{-1}&0\\0&\lambda\end{pmatrix}^{-1}=\begin{pmatrix}1&0\\\lambda^2&1\end{pmatrix}\in\mathfrak{N}'$$

对一切$\lambda\in F^*$。进而有

$$\begin{pmatrix}1&\lambda^2\\0&1\end{pmatrix}\begin{pmatrix}1&\\-\lambda^2&1\end{pmatrix}\begin{pmatrix}0&1\\1&0\end{pmatrix}\begin{pmatrix}1&0\\\lambda^2&1\end{pmatrix}=\begin{pmatrix}\lambda^2&0\\0&\lambda^{-2}\end{pmatrix}\in\mathfrak{N}'$$

对一切$\lambda\in F^*$。考虑

$$\begin{pmatrix}1&\lambda\\0&1\end{pmatrix}\begin{pmatrix}\lambda^2&0\\0&\lambda^{-2}\end{pmatrix}\begin{pmatrix}1&\lambda\\0&1\end{pmatrix}^{-1}\begin{pmatrix}\lambda^2&0\\0&\lambda^{-2}\end{pmatrix}^{-1}=\begin{pmatrix}1&\lambda+\lambda^5\\0&1\end{pmatrix}$$

得到$T_{12}(\lambda+\lambda^5)\in\mathfrak{N}'$，对一切$\lambda\in F^*$。若$\lambda\neq1$，计算

$$\begin{pmatrix}(\lambda+1)^2&0\\0&(\lambda+1)^{-2}\end{pmatrix}^{-1}\begin{pmatrix}1&\lambda+\lambda^5\\0&1\end{pmatrix}$$

$$\cdot\begin{pmatrix}(\lambda+1)^2&0\\0&(\lambda+1)^{-2}\end{pmatrix}=\begin{pmatrix}1&\lambda\\0&1\end{pmatrix},$$

因此$\mathfrak{N}'\ni T_{12}(\lambda)$，对一切$\lambda\neq1$。又已知$\mathfrak{N}'\ni T_{12}(1)$，于是$\mathfrak{N}'\ni T_{12}(\lambda)$，对一切$\lambda\in F$。再由

$$\begin{pmatrix}0&1\\1&0\end{pmatrix}\begin{pmatrix}1&\mu\\0&1\end{pmatrix}\begin{pmatrix}0&1\\1&0\end{pmatrix}^{-1}=\begin{pmatrix}1&0\\\mu&1\end{pmatrix},$$

得到$\mathfrak{N}'\supseteq SL_2(F)$，引理得证。

定理5.1.5 设$n\geqslant2$，$\mathfrak{N}$是$GL_n(F)$的子群，而且$\mathfrak{N}$在$SL_n(F)$之下不变，则除了$n=2$，$|F|=2$和3的情形，$\mathfrak{N}$或者是$GL_n(F)$中心的一个子群，或者$\mathfrak{N}\supseteq SL_n(F)$。

证明 首先假设 $n\geqslant 3$。若$\mathfrak{N}$不是$GL_n(K)$中心的一个子群，则有一元素$A\in\mathfrak{N}\setminus C(GL_n(K))$，和存在一元素$B=T_{ij}(\lambda)$，使得$AB\neq BA$。考虑$B^{-1}A^{-1}BA=T$，因$\mathfrak{N}$在$SL_n(K)$之下不变，故$T\in\mathfrak{N}$。写$B=I+\lambda E_{ij}$，$E_{ij}^2=0$，$\operatorname{rank}(E_{ij})=1$。把$B$代入计算$T$：

$$T=(I-\lambda E_{ij})A^{-1}(I+\lambda E_{ij})A$$
$$=I+A^{-1}E_{ij}A-E_{ij}A^{-1}(I+E_{ij})A。$$

令$S=A^{-1}E_{ij}A-E_{ij}A^{-1}(I+E_{ij})A$，则$T=I+S$，$S\neq 0$，易见$\operatorname{rank}(A^{-1}E_{ij}A)=1$，$\operatorname{rank}(E_{ij}A^{-1}(I+E_{ij})A)\leqslant 1$，因此$\operatorname{rank}S\leqslant 2$。由线性代数的基础知识可知，存在$P\in SL_n(K)$，使得

$$PSP^{-1}=\begin{pmatrix} U^{(2,n)} \\ 0^{(n-2,n)} \end{pmatrix}。$$

于是

$$T_1=PTP^{-1}=P(I+S)P^{-1}=\begin{pmatrix} A_1^{(2)} & B_1 \\ 0 & I^{(n-2)} \end{pmatrix}\in\mathfrak{N}。$$

由此，可假设$\mathfrak{N}$包有形如

$$D=\begin{pmatrix} I^{(2)} & N^{(2,n-2)} \\ 0 & I^{(n-2)} \end{pmatrix}$$

的元素。因为若$A_1^{(2)}\neq I^{(2)}$，那么由于

$$\begin{pmatrix} A_1^{(2)} & B_1 \\ 0 & I^{(n-2)} \end{pmatrix}\begin{pmatrix} I^{(2)} & X \\ 0 & I^{(n-2)} \end{pmatrix}\begin{pmatrix} A_1^{(2)} & B_1 \\ 0 & I^{(n-2)} \end{pmatrix}^{-1}\begin{pmatrix} I^{n} & X \\ 0 & I^{(n-2)} \end{pmatrix}^{-1}$$
$$=\begin{pmatrix} I^{(2)}) & A_1-I)X \\ 0 & I^{(n-2)} \end{pmatrix}\in\mathfrak{N},$$

对任何X。选取X，使得$(A_1^{(2)}-I^{(2)})X\neq 0$，就得到形如$D$的元素。下面分两种情况讨论。

（1）$\operatorname{rank}N^{(2,n-2)}=2$。

存在 $Q_1 \in GL_2(F)$ 和 $Q_2 \in GL_{n-2}(F)$，使得 $Q_1NQ_2^{-1}$ $=\begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \end{pmatrix}$。因此，可选取 $Q_1 \in SL_2(K)$ 和 $Q_2 \in SL_{n-2}(K)$，使得

$$Q_1NQ_2^{-1}=\begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & \lambda & 0 & \cdots & 0 \end{pmatrix}, \quad \lambda \neq 0.$$

由于 $\mathrm{rank}N=2$，必有 $n \geqslant 4$。为简单起见，对 $n=4$ 写出下面的元素：

$$\begin{pmatrix} 1 & -1 & 0^{(2)} \\ 0 & 1 & \\ 0^{(2)} & & I^{(2)} \end{pmatrix}\begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & \lambda \\ 0^{(2)} & & I^{(2)} & \end{pmatrix}\begin{pmatrix} 1 & -1 & 0^{(2)} \\ 0 & 1 & \\ 0^{(2)} & & I^{(2)} \end{pmatrix}^{-1}$$

$$\cdot\begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & \lambda \\ 0^{(2)} & & I^{(2)} & \end{pmatrix}^{-1}=\begin{pmatrix} 1 & 0 & 0 & -\lambda \\ 0 & 1 & 0 & 0 \\ 0^{(2)} & & I^{(2)} & \end{pmatrix} \in \mathfrak{N}$$

是一平延，由引理5.1.1，$\mathfrak{N} \supseteq SL_n(K)$

（2）$\mathrm{rank}N=1$。

此时，D就是一平延，仍由引理5.1.1，$\mathfrak{N} \supseteq SL_n(K)$。

下面讨论 $n=2$ 的情况，采用参考文献〔6〕中给出的证明。

（1）如果 $\mathfrak{N} \subsetneq C(GL_2(K))$，则 $\mathfrak{N}$ 包有形如

$$\begin{pmatrix} 0 & b \\ c & d \end{pmatrix}$$

的元素。设 $A=\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathfrak{N} \setminus C(GL_2(K))$，则

$$\begin{pmatrix} 1 & 0 \\ \lambda & 1 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 1 & 0 \\ \lambda & 1 \end{pmatrix}^{-1}=\begin{pmatrix} a-b\lambda & * \\ * & * \end{pmatrix} \in \mathfrak{N},$$

对一切 $\lambda \in K$，

其中 $*$ 表示域 K 中的某个元素。如果 $b \neq 0$，取 $\lambda=b^{-1}a$ 便得到（1）。如果 $b=0$，则 $\mathfrak{N}$ 包有

$$\begin{pmatrix}1 & \lambda\\0 & 1\end{pmatrix}\begin{pmatrix}a & 0\\c & d\end{pmatrix}\begin{pmatrix}1 & \lambda\\ & 1\end{pmatrix}^{-1}=\begin{pmatrix}a+\lambda c & *\\ * & *\end{pmatrix},$$

对一切 $\lambda\in K$,

如果 $c\neq 0$，取 $\lambda=-c^{-1}a$ 便得到（1）。如果 $c=b=0$，则 $\mathfrak{N}$ 包有

$$\begin{pmatrix}1 & 1\\0 & 1\end{pmatrix}\begin{pmatrix}a & 0\\0 & d\end{pmatrix}\begin{pmatrix}1 & 1\\0 & 1\end{pmatrix}^{-1}=\begin{pmatrix}a & d-a\\0 & d\end{pmatrix},$$

若 $a=d$，与 $A\notin C(GL_2(K))$ 矛盾。因此 $a\neq d$，这就化为前面已讨论过的情形。

（2）如果 $|K|\neq 2, 3, 5$，则 $\mathfrak{N}$ 一定包有一个形如 $\begin{pmatrix}a & b\\0 & d\end{pmatrix}$ 的元素，其中 $a\neq d$。

设 $\mathfrak{N}$ 包有形如 $\begin{pmatrix}0 & b\\c & d\end{pmatrix}$ 的元素，则 $\mathfrak{N}$ 包有

$$\begin{pmatrix}0 & b\\c & d\end{pmatrix}^{-1}\begin{pmatrix}\lambda & 0\\0 & \lambda^{-1}\end{pmatrix}^{-1}\begin{pmatrix}0 & b\\c & d\end{pmatrix}\begin{pmatrix}\lambda & 0\\0 & \lambda^{-1}\end{pmatrix}=\begin{pmatrix}\lambda^2 & *\\0 & \lambda^{-2}\end{pmatrix},$$

由于 $|K|\neq 2, 3, 5$，可选取 λ，使得 $\lambda^2\neq\lambda^{-2}$。于是 $\mathfrak{N}$ 包有 $\begin{pmatrix}\lambda^2 & *\\0 & \lambda^{-2}\end{pmatrix}$，$\lambda^2\neq-\lambda^{-2}$。

（3）如果 $|K|=5$，由（1），可假设 $\mathfrak{N}$ 包有 $\begin{pmatrix}0 & b\\c & d\end{pmatrix}$，进而可假定 $c=-b^{-1}$。不然的话，$\mathfrak{N}$ 包有

$$\begin{pmatrix}1 & 1\\0 & 1\end{pmatrix}\begin{pmatrix}0 & b\\c & d\end{pmatrix}\begin{pmatrix}1 & 1\\0 & 1\end{pmatrix}^{-1}\begin{pmatrix}0 & b\\c & d\end{pmatrix}^{-1},$$

这是一个行列式为 1 的非中心元素，从这个元素出发，利用（1）中的方法，可得到形如 $\begin{pmatrix}0 & b\\-b^{-1} & d\end{pmatrix}$ 的元素包含在 $\mathfrak{N}$ 中。不妨假设

$d \neq 0$。否则$\mathfrak{N}$包有

$$\begin{pmatrix} 0 & b \\ -b^{-1} & 0 \end{pmatrix}^{-1} \begin{pmatrix} 2 & 0 \\ b^{-1} & 2^{-1} \end{pmatrix}^{-1} \begin{pmatrix} 0 & b \\ -b^{-1} & 0 \end{pmatrix} \begin{pmatrix} 2 & 0 \\ b^{-1} & 2^{-1} \end{pmatrix}$$

$$= \begin{pmatrix} 0 & 2^{-1}b \\ 2^{-1}b^{-1} & -1 \end{pmatrix}。$$

注意，$-2^{-1} \equiv 2 \pmod 5$。因此不妨设$\mathfrak{N}$包有$\begin{pmatrix} 0 & b \\ -b^{-1} & d \end{pmatrix}$，$d \neq 0$。于是$\mathfrak{N}$包有

$$\left[\begin{pmatrix} 0 & b \\ -b^{-1} & d \end{pmatrix}^{-1} \begin{pmatrix} 2 & 0 \\ 0 & 2^{-1} \end{pmatrix}^{-1} \begin{pmatrix} 0 & b \\ -b^{-1} & d \end{pmatrix} \begin{pmatrix} 2 & 0 \\ 0 & 2^{-1} \end{pmatrix}\right]^2$$

$$= \begin{pmatrix} 1 & -bd \\ 0 & 1 \end{pmatrix}, \qquad bd \neq 0。$$

由引理5.1.1，$\mathfrak{N} \supseteq SL_2(K)$。

当$|F| = 2$和3时，本定理不成立。当$|F| = 2$时，用F_2表示，有$GL_2(F_2) \cong SL_2(F_2) \cong S_3$(三个文字的对称群)。$S_3$包有非中心正规子群$\mathfrak{A}_3$(交错群)。当$|F| = 3$时，用$F_3$表示，则$SL_2(F_3)$由下面的24个元素组成：

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix},$$

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & -1 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix},$$

$$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ -1 & -1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 1 & -1 \end{pmatrix},$$

$$\begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}, \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix},$$

$$\begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix},$$

$$\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \begin{pmatrix} -1 & -1 \\ -1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & -1 \\ -1 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 1 \\ 1 & 1 \end{pmatrix}.$$

可以验证下面的 8 个元素：

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix},$$

$$\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \begin{pmatrix} -1 & -1 \\ -1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & -1 \\ -1 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 1 \\ 1 & 1 \end{pmatrix}$$

组成 $SL_2(F_3)$ 的一个正规子群。

定理 5.1.5 有下面的推论。

定理5.1.6 设 $n \geqslant 2$，则除非 $n=2$ 及 $F=F_2$ 或 F_3，$PSL_n(K)$ 是单群。

定理5.1.7 设 $n \geqslant 2$，则除非 $n=2$ 及 $F=F_2$ 或 F_3，$GL_n(K)$ 的任何正规子群，如不包含在中心之中，必包含 $SL_n(K)$。

§5.2 双线性型

设 V 是域 F 上的有限维线性空间，V^* 是 V 的对偶空间或共轭空间，它是由 V 上的线性函数全体组成。从线性代数的知识可知，线性空间 V 上的一个双线性型 B 是指由 $V\times V$ 到域 F 的映射，它将 $(\boldsymbol{x}, \boldsymbol{y}) \in V\times V$ 映到 $B(\boldsymbol{x}, \boldsymbol{y}) \in F$，满足性质：(a) 对任何 $\boldsymbol{y} \in V$，映射 $y_R: \boldsymbol{x} \to B(\boldsymbol{x}, \boldsymbol{y})$ 是 V 上的线性函数；(b) 对任何 $\boldsymbol{x} \in V$，映射 $x_L: \boldsymbol{y} \to B(\boldsymbol{x}, \boldsymbol{y})$ 也是 V 上的线性函数。这两个性质合起来可用下面的式子表示：

$$B(a_1\boldsymbol{x}_1 + a_2\boldsymbol{x}_2, \ b_1\boldsymbol{y}_1 + b_2\boldsymbol{y}_2) = \sum_{i,\ j=1}^{2} a_i b_j B(\boldsymbol{x}_i, \ \boldsymbol{y}_j) \tag{5-5}$$

式 (5-5) 可扩充为

$$B\left(\sum_{i=1}^{n} a_i x_i,\quad \sum_{j=1}^{n} b_j y_j\right)=\sum_{i,\ j=1}^{n} a_i b_j B(x_i,\ y_j) \tag{5-6}$$

式（5-6）实际上给出了一个构造双线性型的方法。设（e_1，…，e_n）是V的基底。对每个指标（i，j），$1 \leqslant i$，$j \leqslant n$，选定一个元素$b_{ij} \in F$与之对应。如果$x=\sum_{i=1}^{n} a_i e_i$，$y=\sum_{i=1}^{n} b_i e_i$，用 $B(x,\ y)=\sum_{i,\ j=1}^{n} a_i b_j b_{ij}$ 定义$V \times V$到F的映射B。容易验证，上面定义的映射B是V上的一个双线性型。另一方面，由式(5-6)可以看出，每个双线性型都可用这种方式得到。由双线性型和基底(e_1，…，e_n)决定的矩阵（$B(e_i,\ e_j)$)称为B相对基底(e_1,…,e_n)的阵表示，此阵的行列式 $\det(B(e_i,\ e_j))$ 称为B的**判别式**。显然，双线性型B相对V的不同基底所得的阵表示是不同的。设(f_1，…，f_n）是V的另一基底和$f_i=\sum_{j=1}^{n} p_{ij} e_j$，$P=(p_{ij})$。有

$$B(f_i,\ f_j)=B\left(\sum_{k=1}^{n} p_{ik} e_k,\quad \sum_{l=1}^{n} p_{jl} e_l\right)$$

$$=\sum_{k,\ l} p_{ik} B(e_k,\ e_l) p_{jl},$$

由此得出B相对基底（f_1，…，f_n）的阵表示为PbP'，其中P'表示阵P的转置矩阵，而$b=(B(e_i,\ e_j))$。即B相对不同基底的阵表示是**合同的**。

设U是V的子空间，B是V上的双线性型。定义

$U^{\perp_L}=\{v \in V \mid B(v,\ u)=0$，对所有 $u \in U\}$，

$U^{\perp_R}=\{v \in V \mid B(u,\ v)=0$，对所有 $u \in U\}$。

显然，$U^{\perp_L}$和$U^{\perp_R}$都是V的子空间。特别，子空间$V^{\perp_L}$和$V^{\perp_R}$分别称为V相对B的**左根**和**右根**。

定理5.2.1 下面关于双线性型B的三个条件是等价的：(a) $V^{\perp_R}=0$，(b) $V^{\perp_L}=0$，(c) B相对V的任何基底的阵都是可逆的。

证明 设$(e_1, \cdots, e_n)$是V的基底。$B(e_i, e_j)=b_{ij}$，先证明(a)与(c)等价。

条件$V^{\perp_R}=0$是说，如果向量v对于空间V的任何向量w都有$B(w, v)=0$，则$v=0$。这等价于，如果$B(e_i, v)=0$，对每个基元e_i，则$v=0$。设$v=\sum_{i=1}^{n} c_ie_i$，那么上面条件等价于线性齐次方程组

$$B(e_i, v)=\sum_{j=1}^{n} c_jB(e_i, e_j)=0,$$

$$i=1, 2, \cdots, n。$$

设有非零群，而这条件等价于矩阵$(B(e_i, e_j))$是可逆的。于是得到(a)与(c)等价。同样可证(b)与(c)等价。

一个双线性型B称为**非退化的**，如果它满足定理5.2.1的任何一个条件。

命题5.2.1 B是V上非退化的双线性型当且仅当对于V上的每个线性函数都存在一个向量$x\in V$，使得此函数具有形式x_R: $y\to B(y, x)$；当且仅当对于V上的每个线性函数都存在一个向量$y\in V$，使得此函数具有形式y_L: $x\to B(x, y)$。

证明 考虑由V到V^*的映射$R: x\to x_R$。易知，R是线性映射。$x\in \mathrm{Ker}(R)$当且仅当$x\in V^{\perp_R}$。如果B是非退化的，$V^{\perp_R}=0$。因此$\mathrm{Ker}(R)=0$，R是一一的。再由于$\dim V=\dim V^*$，则R是映上。若R是映上，由于$\dim V=\dim V^*$，R必是一一的。$\mathrm{Ker}(R)=0$，即$V^{\perp_R}=0$，B是非退化的。于是得到了命题所述的第一部分。关于第二部分证明与此完全相同，请读者证明。

命题5.2.2 设B是V上非退化的双线性型，U是V的子空间，那么

（1）U上的任何线性函数有形式$y\to B(x, y)$，对某个$x\in V$；也具有形式$y\to B(y, x)$，对某个$x\in V$。

（2）$\dim U^{\perp_R}=n-\dim U=\dim U^{\perp_L}$。

（3）$(U^{\perp_R})^{\perp_L}=U=(U^{\perp_L})^{\perp_R}$。

证明 （1）对于$x\in V$，$x_R\in V^*$。将x_R限制到子空间U上，则$x_R|U$可以看作U上的线性函数。映射$x\to x_R|U$是V到U^*的映射，此映射的核是$U^{\perp_R}$。令W表示此映射的像，即W是U上具有形式$y\to B(y, x)$的线性函数的集合。现证明$W=U^*$。令g是U上的线性函数，那么可以将g线性扩张为V上的线性函数g'。选取V的基底$(f_1, \cdots, f_n)$，使得$(f_1, \cdots, f_r)$是U的基底，这由线性代数中的替换定理保证可行。由命题5.2.1，g'可具有形式$y\to B(y, x)$，对某个$x\in V$。但是$g'|U=g$，故g也具有上面的形式，因此$W=U^*$。这就得到了（1）的一部分结论，而另一部分则仿此同样可得。

（2）
$$n=\dim V=\dim U^{\perp_R}+\dim W=\dim U^{\perp_R}+\dim U^*$$
$$=\dim U^{\perp_R}+\dim U。$$

于是
$$\dim U^{\perp_R}=n-\dim U。$$

同样可证
$$\dim U^{\perp_L}=n-\dim U。$$

（3）$\dim(U^{\perp_L})^{\perp_R}=n-\dim U^{\perp_L}=n-(n-\dim U)=U$。另一方面，由$U^{\perp_L}$和$U^{\perp_R}$的定义有$(U^{\perp_L})^{\perp_R}\supseteq U$，因此$(U^{\perp_L})^{\perp_R}=U$。同样可证$(U^{\perp_R})^{\perp_L}=U$。

对于双线性型B，若$B(\boldsymbol{x}, \boldsymbol{y})=B(\boldsymbol{y}, \boldsymbol{x})$，对所有$\boldsymbol{x}, \boldsymbol{y}\in V$都成立，则称$B$为**对称双线性型**；若$B(\boldsymbol{x}, \boldsymbol{x})=0$，对所有$x\in V$都成立，则称$B$为**交错双线性型**或简称为**交错型**。对于$\boldsymbol{x}, \boldsymbol{y}\in V$，如果$B(\boldsymbol{x}, \boldsymbol{y})=0$，则说$\boldsymbol{x}$相对于$B$正交于$\boldsymbol{y}$。注意，从定义来看，这并不能推出$B(\boldsymbol{y}, \boldsymbol{x})=0$，即一般说来，

正交关系并不对称。但是在实际上，有兴趣的则是具有对称性的正交关系。

定理5.2.2 设B是V上的双线性型。那么由B定义的正交关系是对称的，当且仅当或者B是对称的，即$B(\boldsymbol{x},\ \boldsymbol{y})=B(\boldsymbol{y},\ \boldsymbol{x})$，对所有的$\boldsymbol{x},\ \boldsymbol{y}\in V$；或者$B$是交错的，即$B(\boldsymbol{x},\ \boldsymbol{x})=0$，对所有的$\boldsymbol{x}\in V$。

证明 若B是对称的，显然B定义的正交关系是对称的。若B是交错的，那么由

$$B(\boldsymbol{x}+\boldsymbol{y},\ \boldsymbol{x}+\boldsymbol{y})=B(\boldsymbol{x},\ \boldsymbol{x})+B(\boldsymbol{x},\ \boldsymbol{y})+B(\boldsymbol{y},\ \boldsymbol{x})+B(\boldsymbol{y},\ \boldsymbol{y})$$

及

$$B(\boldsymbol{x}+\boldsymbol{y},\ \boldsymbol{x}+\boldsymbol{y})=B(\boldsymbol{x},\ \boldsymbol{x})=B(\boldsymbol{y},\ \boldsymbol{y})=0$$

得到

$$B(\boldsymbol{x},\ \boldsymbol{y})=-B(\boldsymbol{y},\ \boldsymbol{x}),$$

于是B定义的正交关系也是对称的。

反之，若B定义的正交关系是对称的。令$\boldsymbol{x},\ \boldsymbol{y},\ \boldsymbol{z}$是$V$中任意三个向量，并令$\boldsymbol{w}=B(\boldsymbol{x},\ \boldsymbol{y})\boldsymbol{z}-B(\boldsymbol{x},\ \boldsymbol{z})\boldsymbol{y}$，则$B(\boldsymbol{x},\ \boldsymbol{w})=0$。于是根据$B$的假设条件，$B(\boldsymbol{w},\ \boldsymbol{x})=0$。这等价于对任意$\boldsymbol{x},\ \boldsymbol{y},\ \boldsymbol{z}\in V$，

$$B(\boldsymbol{x},\ \boldsymbol{y})B(\boldsymbol{z},\ \boldsymbol{x})-B(\boldsymbol{x},\ \boldsymbol{z})B(\boldsymbol{y},\ \boldsymbol{x})=0 \qquad (5\text{-}7)$$

取$\boldsymbol{x}=\boldsymbol{y}$，则对$V$中任何$\boldsymbol{x},\ \boldsymbol{z}$，有

$$B(\boldsymbol{x},\ \boldsymbol{x})(B(\boldsymbol{z},\ \boldsymbol{x})-B(\boldsymbol{x},\ \boldsymbol{z}))=0 \qquad (5\text{-}8)$$

可以断言，对V中任何$\boldsymbol{x},\ \boldsymbol{z}$，或者$B(\boldsymbol{x},\ \boldsymbol{z})=B(\boldsymbol{z},\ \boldsymbol{x})$，或者$B(\boldsymbol{x},\ \boldsymbol{x})=0$。如果不然，则存在$\boldsymbol{x}_1,\ \boldsymbol{y}_1,\ \boldsymbol{z}_1$，使得$B(\boldsymbol{x}_1,\ \boldsymbol{x}_1)\neq 0$和$B(\boldsymbol{y}_1,\ \boldsymbol{z}_1)\neq B(\boldsymbol{z}_1,\ \boldsymbol{y}_1)$。根据式(5-8)，得到$B(\boldsymbol{y}_1,\ \boldsymbol{y}_1)=B(\boldsymbol{z}_1,\ \boldsymbol{z}_1)=0$和$B(\boldsymbol{x}_1,\ \boldsymbol{y}_1)=B(\boldsymbol{y}_1,\ \boldsymbol{x}_1)$，$B(\boldsymbol{x}_1,\boldsymbol{z}_1)=B(\boldsymbol{z}_1,\ \boldsymbol{x}_1)$。由式(5-7)得到$B(\boldsymbol{x}_1,\ \boldsymbol{y}_1)=B(\boldsymbol{y}_1,\ \boldsymbol{x}_1)=0$，$B(\boldsymbol{x}_1,\ \boldsymbol{z}_1)=B(\boldsymbol{z}_1,\ \boldsymbol{x}_1)=0$。再由式(5-8)，$B(\boldsymbol{x}_1+\boldsymbol{z}_1,\boldsymbol{x}_1+\boldsymbol{z}_1)=0$。但是

$$B(\boldsymbol{x}_1+\boldsymbol{z}_1,\ \boldsymbol{x}_1+\boldsymbol{z}_1)=B(\boldsymbol{x}_1,\ \boldsymbol{x}_1)+B(\boldsymbol{x}_1,\ \boldsymbol{y}_1)$$
$$+B(\boldsymbol{z}_1,\ \boldsymbol{x}_1)+B(\boldsymbol{z}_1,\ \boldsymbol{z}_1) \qquad (5\text{-}9)$$

于是$B(\boldsymbol{x}_1,\ \boldsymbol{x}_1)=0$，这与$\boldsymbol{x}_1$的选取矛盾。证毕。

本章以下各节，只考虑正交关系对称的双线性型，即只考虑对称双线性型和交错双线性型。这两种情形，对任何子空间U，都有$U^{\perp_R}=U^{\perp_L}$。用$U^{\perp}$表示U的正交子空间，而不再区分左正交与右正交。通常称$U^{\perp}$为U的**正交补**。V上的双线性型B限制在子空间U上，得到U上的双线性型$B|U$。$B|U$在U上是非退化的，当且仅当$U\cap U^{\perp}=\{\mathbf{0}\}$。若$B|U$是非退化的，则称$U$是非退化的子空间，这时有

$$V=U\oplus U^{\perp}。$$

下面分别讨论交错型和对称型。

§5.3 交 错 型

在§5.2中已经看到，如果B是交错的，则B是斜对称的，即$B(\boldsymbol{x},\ \boldsymbol{y})=-B(\boldsymbol{y},\ \boldsymbol{x})$，对所有的$\boldsymbol{x}$和$\boldsymbol{y}$，这时$B$相应的阵是斜对称矩阵。进而，如果域的特征$\neq 2$，则$B$是交错的，当且仅当$B$是斜对称的。因而在复数域和实数域上，只有斜对称的概念，因为它们都是特征为零的域。如果$n\times n$阵是斜对称的，而且主对角线上的元素都是0，则它是**交错阵**。对于空间V任意选定一基底，双线性型B是交错的，当且仅当它相对给定基底的阵是交错的。交错双线性型的结构非常简单，它由下面的定理给出。

定理5.3.1 如果B是空间V上的交错双线性型，则存在V的一个基底$(\boldsymbol{u}_1,\ \boldsymbol{v}_1,\ \cdots,\ \boldsymbol{u}_r,\ \boldsymbol{v}_r,\ \boldsymbol{z}_1,\ \cdots,\ \boldsymbol{z}_{n-2r})$，使得$B$相对这个基底的阵表示有形式

$$\begin{pmatrix} S & & & & & \\ & S & & & & \\ & & \ddots & & & \\ & & & S & & \\ & & & & 0 & & \\ & & & & & \ddots & \\ & & & & & & 0 \end{pmatrix} \begin{matrix} \left.\right\} r\text{个} \\ \left.\right\} n-2r \end{matrix}$$

其中 $S=\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$。

证明 如果$B=0$，即$B(\boldsymbol{x}, \boldsymbol{y})=0$，对所有$\boldsymbol{x}$, $\boldsymbol{y}$，定理显然成立。如果$B\neq 0$，那么一定存在两个向量$\boldsymbol{u}_1$和$\boldsymbol{v}_1$，使得$B(\boldsymbol{u}_1, \boldsymbol{v}_1)\neq 0$。不失一般性，可设$B(\boldsymbol{u}_1, \boldsymbol{v}_1)=1$。不难看出，由于$B$是交错型，$\boldsymbol{u}_1$和$\boldsymbol{v}_1$是线性无关的。令$V_1$是由$\boldsymbol{u}_1$和$\boldsymbol{v}_1$张成的子空间。可证明$V=V_1\oplus V_1^{\perp}$。为此，只要证明$^B|_{V_1}$是非退化的就行。$^B|_{V_1}$相对$V_1$的基底$(\boldsymbol{u}_1, \boldsymbol{v}_1)$的阵表示为$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}=S$是可逆的。因而$^B|_{V_1}$是非退化的。令$^B|_{V^{\perp}}=B_1$，对$B_1$作与上面相同的讨论，或者$B_1=0$，这时$r=1$；或者$B_1\neq 0$，在$V_1^{\perp}$中存在$\boldsymbol{u}_2$, $\boldsymbol{v}_2$，使得$B_1(\boldsymbol{u}_2, \boldsymbol{v}_2)=1$。令$V_2$是由$\boldsymbol{u}_2$, $\boldsymbol{v}_2$张成的子空间，$V_2\subset V_1^{\perp}$，于是有$V=V_1\oplus V_2\oplus(V_1\oplus V_2)^{\perp}$。按此步骤继续下去，有限步以后便得到定理。

对矩阵运算有兴趣的读者，不妨试用纯矩阵运算证明本定理。

系5.3.1 在定理5.3.1中，将基底重新排列为$(\boldsymbol{u}_1, \boldsymbol{u}_2, \cdots, \boldsymbol{u}_r, \boldsymbol{v}_1, \cdots, \boldsymbol{v}_r, \boldsymbol{z}_1, \cdots, \boldsymbol{z}_{n-2r})$，则交错型$B$相应的阵表示是

$$\begin{pmatrix} 0 & I^{(r)} & \\ -I^{(r)} & 0 & \\ & & 0^{(n-2r)} \end{pmatrix}。\tag{5-10}$$

系5.3.2 域上交错阵的秩是偶数，其行列式是域中平方元。一个交错阵的秩若为$2r$，则它合同于形如式(5-10)的阵。因此，两个交错阵合同当且仅当它们有相同的秩。

系5.3.3 设(a_{ij})是交错阵，$f(\boldsymbol{x}, \boldsymbol{y})=\sum\limits_{i,j=1}^{n} a_{ij}x_iy_j$给出$V\times V\to F$的映射，其中$\boldsymbol{x}=\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$，$\boldsymbol{y}=\begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}$。那么存

在可逆线性变换$P=(p_{ij})$，令

$$x'_i=\sum_{k=1}^{n} x_k p_{ki},$$

$$y'_j=\sum_{l=1}^{n} y_l p_{lj},$$

得到$f(\boldsymbol{x},\ \boldsymbol{y})$的简化形式：

$$f(\boldsymbol{x},\ \boldsymbol{y})=(x'_1y'_2-x'_2y'_1)+\cdots+(x'_{2r-1}y'_{2r}-x'_{2r}y'_{2r-1})。$$

§5.4 辛　　群

5.4.1　辛群的定义

域F上的有限维线性（向量）空间V和它上面的非退化的交错双线性型B称为**辛空间**。由前面的讨论可知，辛空间的维数必定是偶数。V上的可逆线性变换$\eta\in GL(V)$，若对所有的$\boldsymbol{x}$、$\boldsymbol{y}\in V$，满足$B(\eta(\boldsymbol{x}),\ \eta(\boldsymbol{y}))=B(\boldsymbol{x},\ \boldsymbol{y})$，则称之为**辛映射**或**辛变换**。$V$上辛变换全体组成一群，称为**辛群**，用$Sp_n(F,\ B)$表示。其中$n=\dim V$。在$V$中选定一基底，将交错型B对应的阵表示仍记为$B$。$n\times n$阵$M\in GL_n(F)$称为**辛阵**。如果它满足$B=MBM'$，$\eta\in GL_n(V)$是辛变换，当且仅当$\eta$对应的阵表示$M$是辛阵。事实上，辛群在同构的意义下只有1个。因为$V$上任何一个非退化交错型都合同于$B_1=\begin{pmatrix}0 & I^{(r)}\\ -I^{(r)} & 0\end{pmatrix}$，$n=2r$。对于非退化交错型$B$，存在可逆矩阵$P\in GL_n(F)$，使得$B_1=PBP'$。令$\Psi$是由辛群$Sp_n(F,\ B)$到$Sp_n(F,\ B_1)$的映射，它将$\eta\in Sp_n(F,\ B)$映到$P\eta P^{-1}\in Sp_n(F,\ B_1)$，易见$\Psi$是群同构映射。因此，可以认为辛群不依赖于$B$，而只依赖于基域和空间的维数，故简记为$Sp_n(F)$。在研究辛群时，总选定$B=\begin{pmatrix}0 & I^{(r)}\\ -I^{(r)} & 0\end{pmatrix}$，$n=2r$。下面用矩阵研究辛群，$Sp_n(F)=\{T\in GL_n(F)\mid B=TBT'\}$。

设 $T=\begin{pmatrix}A & B\\ C & D\end{pmatrix}$，那么 $T\in Sp_n(F)$ 当且仅当

$$\begin{pmatrix}A & B\\ C & D\end{pmatrix}\begin{pmatrix}0 & I^{(r)}\\ -I^{(r)} & 0\end{pmatrix}\begin{pmatrix}A & B\\ C & D\end{pmatrix}'=\begin{pmatrix}0 & I^{(r)}\\ -I^{(r)} & 0\end{pmatrix},$$

此条件等价于

$$\begin{cases}AB'=BA'\\ CD'=DC'\\ AD'-BC'=I\end{cases}\tag{5-11}$$

容易验证，下边三种类型的阵都满足式（5-11），是辛矩阵：

Ⅰ. $\begin{pmatrix}I & S\\ 0 & I\end{pmatrix}$，$S'=S$，$\begin{pmatrix}I & 0\\ T & I\end{pmatrix}$，$T'=T$。

Ⅱ. $\begin{pmatrix}A & 0\\ 0 & (A^{-1})'\end{pmatrix}$，$A\in GL_r(F)$。

Ⅲ. $\begin{pmatrix}J & I-J\\ -(I-J) & J\end{pmatrix}$，$J$ 为对角阵和 $J^2=J$。

称类型Ⅰ的阵为**辛平移**，类型Ⅱ的阵为**辛旋转**，类型Ⅲ的阵为**半对合**。

定理5.4.1 辛群 $Sp_n(F)$ 由一切辛平移，辛旋转和半对合生成。

证明 令 $T=\begin{pmatrix}A & B\\ C & D\end{pmatrix}\in Sp_n(F)$。分二种情形讨论。

（1）$\operatorname{rank}A=r$，即 A 是可逆阵。考虑

$$\begin{pmatrix}A^{-1} & 0\\ 0 & A'\end{pmatrix}\begin{pmatrix}A & B\\ C & D\end{pmatrix}=\begin{pmatrix}I & B_1\\ C_1 & D_1\end{pmatrix}\in Sp_n(F)。$$

由 $I\cdot B_1'=B_1I'$，得到 $B_1=B_1'$。考虑

$$\begin{pmatrix}I & B_1\\ C_1 & D_1\end{pmatrix}\begin{pmatrix}I & -B_1\\ 0 & I\end{pmatrix}=\begin{pmatrix}I & 0\\ C_1 & D_2\end{pmatrix}\in Sp_n(F),$$

由 $I\cdot D_2'=I$ 和$C_2D_2'=D_2C_2'$，得到$D_2=I$ 和 $C_2'=C_2\cdot\begin{pmatrix}I & 0\\ C_2 & D_2\end{pmatrix}=$ $\begin{pmatrix}I & 0\\ C_2 & I\end{pmatrix}\in Sp_n(F)$。综合上述，$T$ 可表成 I，Ⅱ型元素的积。

（2）$\operatorname{rank}A=r_1<r$。这时存在$P$，$Q\in GL_r(F)$，使得

$$PAQ=\begin{pmatrix}I^{(r_1)} & 0^{(r_1,r-r_1)}\\ 0^{(r-r_1,r_1)} & 0^{(r-r_1)}\end{pmatrix}=A_1,$$

这里$C^{(r_1)}$表示$r_1\times r_1$方阵，$C^{(r,r_1)}$表示 $r\times r_1$矩阵。考虑

$$\begin{pmatrix}P & \\ & (P^{-1})'\end{pmatrix}\begin{pmatrix}A & B\\ C & D\end{pmatrix}\begin{pmatrix}Q & \\ & (Q^{-1})'\end{pmatrix}$$

$$=\begin{pmatrix}I^{(r_1)} & 0 & B_1^{(r)}\\ 0 & 0^{(r-r_1)} & \\ \multicolumn{2}{c}{C_1^{(r)}} & D_1^{(r)}\end{pmatrix}\in Sp_r(F)。$$

令

$$B_1=\begin{pmatrix}B_{11}^{(r_1)} & B_{12}^{(r_1,r-r_1)}\\ B_{21}^{(r-r_1,r_1)} & B_{22}^{(r-r_1)}\end{pmatrix},$$

由$A_1B_1'=B_1A_1'$，得到$B_{21}=0$，$B_{11}'=B_{11}$。考虑

$$\begin{pmatrix}I^{(r_1)} & 0 & B_{11} & B_{12}\\ 0 & 0^{(r-r_1)} & 0 & B_{22}\\ \multicolumn{2}{c}{C_1^{(r)}} & \multicolumn{2}{c}{D_1^{(r)}}\end{pmatrix}\begin{pmatrix}I^{(r_1)} & 0 & -B_{11}^{(r_1)} & 0\\ 0 & I^{(r-r_1)} & 0 & 0^{(r-r_1)}\\ \multicolumn{2}{c}{0^{(r)}} & \multicolumn{2}{c}{I^{(r)}}\end{pmatrix}$$

$$=\begin{pmatrix}I^{(r_1)} & 0 & 0 & \widetilde{B}_{12}\\ 0 & 0 & 0 & \widetilde{B}_{22}\\ \multicolumn{2}{c}{C_1^{(r)}} & \multicolumn{2}{c}{D_2^{(r)}}\end{pmatrix}。$$

由于$\operatorname{rank}\begin{pmatrix}I_1^{(r_1)} & 0 & 0 & \widetilde{B}_{12}\\ 0 & 0 & 0 & \widetilde{B}_{22}\end{pmatrix}=r$，有$\widetilde{B}_{22}\in GL_{r-r_1}(F)$。考虑

$$\begin{pmatrix} I_1^{(r_1)} & 0 & 0 & \widetilde{B}_{12} \\ 0 & 0 & 0 & \widetilde{B}_{22} \\ C_1^{(r)} & & D_2^{(r)} & \end{pmatrix}\begin{pmatrix} J & I-J \\ -(I-J) & J \end{pmatrix}$$

$$=\begin{pmatrix} I_1^{(r_1)} & \widetilde{B}_{12} & * \\ 0 & \widetilde{B}_{22} & \\ & * & * \end{pmatrix}\in Sp_n(F),$$

其中 $J=\begin{pmatrix} I_1^{(r_1)} & 0 \\ 0 & 0^{(r-r_1)} \end{pmatrix}$， $I-J=\begin{pmatrix} 0^{(r_1)} & 0 \\ 0 & I^{(r-r_1)} \end{pmatrix}$， * 表示相应的计算结果。由于对其具体结果并不关心，故以 * 代之。在上面的等式中，$\begin{pmatrix} I_1^{(r)} & \widetilde{B}_{12} \\ 0 & \widetilde{B}_{22} \end{pmatrix}$是可逆阵。于是 T 经过Ⅰ，Ⅱ，Ⅲ型元素的左乘或右乘化为情况（1），定理得证。

系5.4.1 $Sp_2(F)=SL_2(F)$。

系5.4.2 若 $T\in Sp_n(F)$，则 $\det T=1$。

定理5.4.2 辛群 $Sp_n(F)$ 的中心 $C(Sp_n(F))=\{I,-I\}$。

证明 设 $T=\begin{pmatrix} A & B \\ C & D \end{pmatrix}\in C(Sp_n(F))$，则

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix}\begin{pmatrix} I & I \\ 0 & I \end{pmatrix}=\begin{pmatrix} I & I \\ 0 & I \end{pmatrix}\begin{pmatrix} A & B \\ C & D \end{pmatrix}。$$

由此有 $C=0$， $A=D$。考虑

$$\begin{pmatrix} A & B \\ 0 & A \end{pmatrix}\begin{pmatrix} I & 0 \\ I & I \end{pmatrix}=\begin{pmatrix} I & 0 \\ I & I \end{pmatrix}\begin{pmatrix} A & B \\ 0 & A \end{pmatrix},$$

可得 $B=0$ 和 $A\cdot A'=I$，于是 $T=\begin{pmatrix} A & 0 \\ 0 & A \end{pmatrix}$， $A=(A')^{-1}$。考虑

$$\begin{pmatrix} A & 0 \\ 0 & A \end{pmatrix}\begin{pmatrix} B & \\ & (B^{-1})' \end{pmatrix}=\begin{pmatrix} B & \\ & (B^{-1})' \end{pmatrix}\begin{pmatrix} A & 0 \\ 0 & A \end{pmatrix},$$

得到 $AB=BA$，对所有 $B\in GL_r(F)$。因此 A 是 $GL_r(F)$ 的中心

元，$A\in C(GL_r(F))$，即$A=\pm I^{(r)}$。于是$T=\pm I^{(n)}$。

5.4.2 子空间在辛群下的可迁性

子空间在辛群作用下的可迁性，是反映了辛空间的几何性质。此外，它对辛群单性的讨论也有重要作用。

设向量空间V的基底为$(e_1, \cdots, e_n)$，U是V的子空间，$\dim U=s$，$(u_1, \cdots, u_s)$是U的基底，其中$u_i=\sum_{j=1}^{n} a_{ij}e_j$，$i=1, 2, \cdots, s$，那么$s\times n$矩阵

$$\begin{pmatrix} u_1 \\ u_2 \\ \vdots \\ u_s \end{pmatrix}=\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{s1} & a_{s2} & \cdots & a_{sn} \end{pmatrix}=(a_{ij})$$

是子空间U的矩阵表示，$\operatorname{rank}(a_{ij})=s$。当然，$U$的阵表示并不唯一。$s\times n$阵$M_1$和$M_2$都是$U$的阵表示，当且仅当存在一个可逆的$s\times s$阵$P\in GL_s(F)$，使得$M_1=PM_2$。注意，通常总是在选定了空间$V$的基底之后才讨论子空间的阵表示。

设U是s维子空间，为简单起见，将U的一个阵表示仍记为U。两个s维子空间U_1和U_2在辛群$Sp_n(F)$下可迁，是指存在$P\in GL_s(F)$和$T\in Sp_n(F)$使得$U_1=PU_2T$。

定理5.4.3 设U_1和U_2是V的两个子空间，则它们在辛群$Sp_n(F)$下可迁当且仅当$\dim U_1=\dim U_2$，并且U_1BU_1'与U_2BU_2'合同，其中$B=\begin{pmatrix} 0 & I^{(r)} \\ -I^{(r)} & 0 \end{pmatrix}$，$n=2r$。

证明 必要性显然。

充分性：设$\dim U_1=\dim U_2=p$，$U_i=(U_{i1}^{(p,r)}, U_{i2}^{(p,r)})$，$i=1, 2$，其中$U_{ij}^{(p,r)}$表示$p\times r$阵。考虑

$$U_i\begin{pmatrix} 0 & I^{(r)} \\ -I^{(r)} & 0 \end{pmatrix}U_i'=(U_{i1}, U_{i2})\begin{pmatrix} 0 & I^{(r)} \\ -I^{(r)} & 0 \end{pmatrix}\begin{pmatrix} U_{i1}' \\ U_{i2}' \end{pmatrix}$$
$$=U_{i1}U_{i2}'-U_{i2}U_{i1}'$$

是$p\times p$的斜对称阵，而且对角线上的元素全是0，故是交错阵。由系5.3.2，存在$p\times p$阵$Q_i\in GL_p(F)$使得

$$Q_iU_i\begin{pmatrix}0 & I^{(r)}\\ -I^{(r)} & 0\end{pmatrix}U_i'Q_i'$$

$$=\begin{pmatrix}0 & I^{(r_i)} & 0^{(r_i,p-2r_i)}\\ -I^{(r_i)} & 0 & 0^{(r_i,p-2r_i)}\\ 0 & 0 & 0^{(p-2r_i)}\end{pmatrix},$$

其中$i=1$，2。由线性代数的知识，可知存在$(n-p)\times n$阵R_i，使得 $\operatorname{rank}\begin{pmatrix}Q_iU_i\\ R_i\end{pmatrix}=2r=n$ （$i=1$，2）。先看$i=1$的情形。这时有

$$\begin{pmatrix}Q_1U_1\\ R_1\end{pmatrix}B\begin{pmatrix}Q_1U_1\\ R_1\end{pmatrix}'$$

$$=\begin{pmatrix}0 & I^{(r_1)} & 0 & B_1^{(2r_1,n-p)}\\ -I^{(r_1)} & 0 & & \\ & 0 & 0^{(p-2r_1)} & B_2^{(p-2r_1,n-p)}\\ & -B_1' & -B_2' & H_2^{(n-p)}\end{pmatrix}$$

令 $H_1=\begin{pmatrix}0 & I^{(r_1)}\\ -I^{(r_1)} & 0\end{pmatrix}$，则

$$\begin{pmatrix}I^{(2r_1)} & 0 & 0\\ 0 & I^{(p-2r_1)} & 0\\ B_1'H_1^{-1} & 0 & I^{(n-p)}\end{pmatrix}\begin{pmatrix}H_1^{(2r_1)} & 0 & B_1\\ 0 & 0^{(p-2r_1)} & B_2\\ -B_1' & -B_2' & H_2^{(n-p)}\end{pmatrix}$$

$$\cdot\begin{pmatrix}I^{(2r_1)} & 0 & 0\\ 0 & I^{(p-2r_1)} & 0\\ B_1'H_1^{-1} & 0 & I^{(n-p)}\end{pmatrix}'=\begin{pmatrix}H_1^{(2r_1)} & 0 & 0\\ 0 & 0^{(p-2r_1)} & B_2\\ 0 & -B_2' & H_3\end{pmatrix},$$

其中$\operatorname{rank}B_2=p-2r_1$。考虑矩阵在相抵变换下的标准型，有$A_1\in GL_{p-2r_1}(F)$和$C_1\in GL_{n-p}(F)$，使得

$$A_1B_2C_1=(I^{(p-2r_1)}\quad 0^{(p-2r_1,n-2p+2r_1)})。$$

于是

$$\begin{pmatrix} I^{(2r_1)} & 0 & 0 \\ 0 & A_1^{(p-2r_1)} & 0 \\ 0 & 0 & C_1'^{(n-p)} \end{pmatrix}\begin{pmatrix} H_1^{(2r_1)} & 0 & 0 \\ 0 & 0^{(p-2r_1)} & B_2 \\ 0 & -B_2' & H_3 \end{pmatrix}$$

$$\cdot\begin{pmatrix} I^{(2r_1)} & 0 & 0 \\ 0 & A_1^{(p-2r_1)} & 0 \\ 0 & 0 & C_1'^{(n-p)} \end{pmatrix}'$$

$$=\begin{pmatrix} I_1^{(2r_1)} & 0 & 0 & 0 \\ 0 & 0^{(p-2r_1)} & I^{(p-2r_1)} & 0^{(p-2r_1,n-2p+2r_1} \\ 0 & -I^{(p-2r_1)} & H_4^{(p-2r_1)} & M \\ 0 & 0 & -M' & H_5^{(n-2p+2r_1)} \end{pmatrix},$$

其中H_4和H_5都是交错阵。令$H_4=T_4-T_4'$，这里

$$T_4=\begin{pmatrix} h_{11} & h_{12} & \cdots & h_{1(p-2r_1)} \\ & h_{22} & \cdots & h_{2(p-2r_1)} \\ & & \ddots & \vdots \\ & 0 & & h_{(p-2r_1)(p-2r_1)} \end{pmatrix}。$$

考虑

$$\begin{pmatrix} I^{(2r_1)} & 0 & 0 & 0 \\ 0 & I^{(p-2r_1)} & 0 & 0 \\ 0 & -T_4 & I^{(p-2r_1)} & 0 \\ 0 & M' & 0 & I^{(n-2p+2r_1)} \end{pmatrix}$$

$$\cdot\begin{pmatrix} H_1^{(2r_1)} & 0 & 0 & 0 \\ 0 & 0^{(p-2r_1)} & I^{(p-2r_1)} & 0 \\ 0 & -I & H_4^{(p-2r_1)} & M \\ 0 & 0 & -M' & H_5 \end{pmatrix}\begin{pmatrix} I^{(2r_1)} & 0 & 0 & 0 \\ 0 & I^{(p-2r_1)} & 0 & 0 \\ 0 & -T_4 & I^{(p-2r_1)} & 0 \\ 0 & M' & 0 & I^{(n-2p+2r_1)} \end{pmatrix}'$$

$$=\begin{pmatrix} H_1^{(2r_1)} & 0 & 0 & 0 \\ 0 & 0^{(p-2r_1)} & I & \\ 0 & -I & 0^{(p-2r_1)} & 0 \\ 0 & 0 & 0 & H_6 \end{pmatrix},$$

其中H_5为交错阵。于是，令

$$T_1=\begin{pmatrix} I^{(2r_1)} & 0 & 0 & 0 \\ 0 & I^{(p-2r_1)} & 0 & 0 \\ 0 & -T_4 & I^{(p-2r_1)} & 0 \\ 0 & M' & 0 & I^{(n-2p+2r_1)} \end{pmatrix}\begin{pmatrix} I^{(2r_1)} & 0 & 0 \\ 0 & A_1^{(p-2r_1)} & 0 \\ 0 & 0 & C_1'^{(n-p)} \end{pmatrix}$$

$$\cdot\begin{pmatrix} I^{(2r_1)} & 0 & 0 \\ 0 & I^{(p-2r_1)} & 0 \\ B_1'H_1^{-1} & 0 & I^{(n-p)} \end{pmatrix}$$

则$T_1\in GL_n(F)$，使得

$$T_1\begin{pmatrix} Q_1U_1 \\ R_1 \end{pmatrix}B\begin{pmatrix} Q_1U_1 \\ R_1 \end{pmatrix}'T_1'$$

$$=\begin{pmatrix} H_1^{(2r_1)} & 0 & 0 & 0 \\ 0 & 0^{(p-2r_1)} & I^{(p-2r_1)} & 0 \\ 0 & -I^{(p-2r_1)} & 0 & 0 \\ 0 & 0 & 0 & H_5^{(n-2p+2r_1)} \end{pmatrix}。$$

对 $i=2$ 作完全同样的讨论，可找到与T_1形状相同的$T_2\in GL_n(F)$，使得

$$T_2\begin{pmatrix} Q_2U_2 \\ R_2 \end{pmatrix}B\begin{pmatrix} Q_2U_2 \\ R_2 \end{pmatrix}'T_2'$$

$$=\begin{pmatrix} H_1^{(2r_2)} & 0 & 0 & 0 \\ 0 & 0^{(p-2r_2)} & I^{(p-2r_2)} & \\ 0 & -I^{(p-2r_2)} & 0 & 0 \\ 0 & 0 & 0 & H_6 \end{pmatrix},$$

其中H_6是交错群。因为U_1BU_1'和U_2BU_2'合同，所以$r_1=r_2$，$\operatorname{rank}H_5=\operatorname{rank}H_6=n-2p+2r_1$。根据系5.3.2，交错阵$H_5$和$H_6$合同。于是存在$R_3\in GL_{n-p}(F)$，使得

$$\begin{pmatrix} I^{(p)} & 0 \\ 0 & R_3^{(n-p)} \end{pmatrix}T_1\begin{pmatrix} Q_1U_1 \\ R_1 \end{pmatrix}B\begin{pmatrix} Q_1U_1 \\ R_1 \end{pmatrix}'T_1'\begin{pmatrix} I^{(p)} & 0 \\ 0 & R_3^{(n-p)} \end{pmatrix}'$$

$$=T_2\begin{pmatrix} Q_2U_2 \\ R_2 \end{pmatrix} B \begin{pmatrix} Q_2U_2 \\ R_2 \end{pmatrix}' T_2',$$

而且

$$T_1\begin{pmatrix} Q_1U_1 \\ R_1 \end{pmatrix}=\begin{pmatrix} \widetilde{A}_1Q_1U_1 \\ \widetilde{R}_1 \end{pmatrix},$$

$$T_2\begin{pmatrix} Q_2U_2 \\ R_2 \end{pmatrix}=\begin{pmatrix} \widetilde{A}_2Q_2U_2 \\ \widetilde{R}_2 \end{pmatrix},$$

其中$\widetilde{A}_i=\begin{pmatrix} I^{(2r_1)} & 0 \\ 0 & A_i^{(p-2r_1)} \end{pmatrix}$，$i=1, 2$。

于是

$$\begin{pmatrix} I & 0 \\ 0 & R_3 \end{pmatrix}\begin{pmatrix} \widetilde{A}_1Q_1U_1 \\ \widetilde{R}_1 \end{pmatrix} B \begin{pmatrix} \widetilde{A}_1Q_1U_1 \\ \widetilde{R}_1 \end{pmatrix}' \begin{pmatrix} I & 0 \\ 0 & R_3 \end{pmatrix}'$$

$$=\begin{pmatrix} \widetilde{A}_2Q_2U_2 \\ \widetilde{R}_2 \end{pmatrix} B \begin{pmatrix} \widetilde{A}_2Q_2U_2 \\ \widetilde{R}_2 \end{pmatrix}'.$$

令

$$P_1=\begin{pmatrix} \widetilde{A}_1Q_1U_1 \\ R_3\widetilde{R}_1 \end{pmatrix},\quad P_2=\begin{pmatrix} \widetilde{A}_2Q_2U_2 \\ \widetilde{R}_2 \end{pmatrix},$$

则

$$P_1BP_1'=P_2BP_2'.$$

于是

$$P_2^{-1}P_1B(P_2^{-1}P_1)'=B,$$

这表明$T=P_2^{-1}P_1\in Sp_n(F)$。因此$P_1=P_2T$，$T\in Sp_n(F)$。考虑P_1和P_2的前p行，有

$$\widetilde{A}_1Q_1U_1=\widetilde{A}_2Q_2U_2T.$$

令$P=Q_1^{-1}\widetilde{A}_1^{-1}\widetilde{A}_2Q_2$，则

$$U_1=PU_2T,$$

其中$P\in GL_p(F)$，$T\in Sp_n(F)$，即子空间U_1和U_2在辛群$Sp_n(F)$下可迁，充分性得证。

系5.4.3 令U_1和U_2是V的两个p维子空间，则存在$T\in Sp_n(F)$使得$U_1=U_2T$的充分必要条件是$U_1BU_1'=U_2BU_2'$。

证明 考察定理5.4.3的证明过程，可发现$Q_1=Q_2$当且仅当$U_1BU_1'=U_2BU_2'$，和由于$\mathrm{rank}B_2=p_1-2r_1$正好等于$B_2$的行数，故可取$A_1=I^{(p-2r_1)}$，同理可取$A_2=I^{(p-2r_1)}$，于是$P=I$，$U_1=U_2T$。

向量$v\in V$称为**迷向的**，如果$vBv'=0$。V的子空间U称为**迷向子空间**，当且仅当UBU'是奇异的。进而，若$UBU'=0$，则称U为**全迷向子空间**。例如，$U=(I^{(r)},\ 0)$就是全迷向子空间。

定理5.4.4 n维向量空间V的全迷向子空间的最大维数是$r=\frac{n}{2}$。

证明 首先，$(I^{(r)},\ 0)$是一个r维的全迷向子空间。设P是一个全迷向子空间，可以断言$\dim P\leqslant r$。用反证法。如果$\dim P>r$，那么考虑

$$\begin{pmatrix} P \\ Q \end{pmatrix} B \begin{pmatrix} P \\ Q \end{pmatrix}' = \begin{pmatrix} 0^{(r_1)} & * \\ * & * \end{pmatrix},$$

其中Q是使$\begin{pmatrix} P \\ Q \end{pmatrix}\in GL_n(F)$的阵，$r_1=\dim P$。将上式右边阵用前$r_1$列作拉普拉斯（Laplace）展开的方法计算行列式，由于$r_1>\frac{n}{2}=r$，此阵的行列式为0，得到矛盾，因此$\dim P\leqslant r$，定理成立。

系5.4.4 极大全迷向子空间在辛群$Sp_n(F)$作用下成一可迁集。

系5.4.5 任意一个全迷向子空间都包含在一个极大全迷向子空间中。

证明 由定理5.4.3可知，维数相同的两个全迷向子空间在

辛群$Sp_n(F)$之下可迁，及s维全迷向子空间$(I^{(s)},\ 0)$包含在极大全迷向子空间$(I^{(r)},\ 0)$之中，其中$s\leqslant r$。综合这两个结果便得到系。

5.4.3 辛平延

平延在讨论线性群时起着重要的作用。对于辛群有相应的辛平延的概念。辛平延在研究辛群的单性时，也起着重要作用。

定理5.4.5 设$T\in Sp_n(F)$，$n=2r$，和$\mathrm{rank}(T-I)=1$，那么

（1）存在向量$\boldsymbol{v}\in V$和$\lambda\in F^*$，使得

$$T=I+\lambda B\boldsymbol{v}'\boldsymbol{v}。$$

（2）$(T-I)^2=0$。

（3）T辛相似于$\begin{pmatrix} I^{(r)} & 0 \\ \begin{matrix}\mu & & \\ & 0 & \\ & & \ddots \\ & & & 0\end{matrix} & I^{(r)} \end{pmatrix}$，$\mu\in F^*$。

证明 （1）由于$\mathrm{rank}(T-I)=1$，则T可表为

$$T=I+\boldsymbol{u}'\boldsymbol{v} \tag{5-12}$$

其中$\boldsymbol{u}$，$\boldsymbol{v}\in V$。由于$T\in Sp_n(F)$，有$TBT'=B$，将式（5-12）代入这个等式，即

$$(I+\boldsymbol{u}'\boldsymbol{v})B(I+\boldsymbol{u}'\boldsymbol{v})'=B \tag{5-13}$$

将式（5-13）展开得到

$$\boldsymbol{u}'\boldsymbol{v}B+B\boldsymbol{v}'\boldsymbol{u}+\boldsymbol{u}'\boldsymbol{v}B\boldsymbol{v}'\boldsymbol{u}=0。 \tag{5-14}$$

直接计算得出$\boldsymbol{v}B\boldsymbol{v}'=0$，于是由式（5-14）得出

$$\boldsymbol{u}'\boldsymbol{v}B=-B\boldsymbol{v}'\boldsymbol{u}=(\boldsymbol{u}'\boldsymbol{v}B)' \tag{5-15}$$

即$\boldsymbol{u}'\boldsymbol{v}B$是对称阵，而且对角线元素有非0元，否则与$\mathrm{rank}(\boldsymbol{u}'\boldsymbol{v}B)=1$矛盾。令

$$\boldsymbol{u}'\boldsymbol{v}B=\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{12} & a_{22} & \cdots & a_{2n} \\ & \cdots & \cdots & \\ a_{1n} & a_{2n} & \cdots & a_{nn} \end{pmatrix},$$

不失一般性，设$a_{11}\neq 0$，则存在$n\times n$可逆阵$P\in GL_n(F)$，使得

$$Pu'vBP'=\begin{pmatrix} a_{11} & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & 0 & \\ 0 & & & \end{pmatrix}$$

于是

$$u'vB=a_{11}P^{-1}\begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}(1 \quad 0 \quad \cdots \quad 0)(P^{-1})'。$$

令$w'=P^{-1}\begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$，直接计算得到$w=\alpha u$，$\alpha\in F^*$。于是

$$u'vB=a_{11}\alpha^2u'u=u'\cdot a_{11}\alpha^2u。$$

由于$u\neq 0$，有$vB=a_{11}\alpha^2u$，$u'=(a_{11}\alpha^2)^{-1}B'v'$。因此

$$T=I+u'\cdot v=I-(a_{11}\alpha^2)^{-1}Bv'v$$
$$=I+\lambda Bv'v,$$

其中$\lambda=-(a_{11}\alpha^2)^{-1}\in F^*$。便得到了（1）。

（2）由（1），$T=I+\lambda Bv'v$。计算

$$(T-I)^2=\lambda^2Bv'vBv'v=0。$$

（3）对任何$v\in V$，$v\neq 0$，都有$vBv'=0$，即任一非0向量都是迷向向量。由定理5.4.3，任何两个非0向量在辛群作用下是可迁的。由（1），$T=I+\lambda Bv'v$，存在辛变换$T_1\in Sp_n(F)$，使得$vT_1=\beta(1, 0\cdots, 0)$，$\beta\in F^*$。考虑

$$T_1^{-1}TT_1=T_1^{-1}(I+\lambda Bv'v)T_1$$
$$=I+\lambda T_1^{-1}B(T_1^{-1})'T_1'v'vT_1$$
$$=I+\lambda B\cdot\beta^2\begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & 0 & \\ 0 & & & \end{pmatrix}=\begin{pmatrix} I^{(r)} & & & 0 \\ \mu & & & \\ & 0 & & I^{(r)} \\ & & \ddots & \\ & & & 0 \end{pmatrix},$$

其中 $\mu=-\lambda\beta^2\in F^*$。得到（3）

对于辛群中元素 $T\in Sp_n(F)$，如果rank$(T-I)=1$，称T为**辛平延**。

定理5.4.6 辛群 $Sp_n(F)$ 由辛平延生成。

证明 已知$Sp_n(F)$ 由下面三类元素生成：

Ⅰ $\begin{pmatrix} I^{(r)} & S \\ 0 & I^{(r)} \end{pmatrix}$，$S'=S$，$\begin{pmatrix} I^{(r)} & 0 \\ T & I^{(r)} \end{pmatrix}$，其中$T'=T$。

Ⅱ $\begin{pmatrix} A & 0 \\ 0 & (A^{-1})' \end{pmatrix}$，其中 $A\in GL_r(F)$。

Ⅲ $\begin{pmatrix} J & I-J \\ -(I-J) & J \end{pmatrix}$，其中$J$为对角阵和$J^2=J$。

为了证明定理，只要证明这三类元素由辛平延生成即可。

（1）
$$\begin{pmatrix} I & S \\ 0 & I \end{pmatrix}=\begin{pmatrix} I & \begin{matrix} s_{11} & & & \\ & 0 & & \\ & & \ddots & \\ & & & 0 \end{matrix} \\ 0 & I \end{pmatrix}\cdot\cdots\cdot\begin{pmatrix} I & \begin{matrix} 0 & & & \\ & \ddots & & \\ & & 0 & \\ & & & s_{rr} \end{matrix} \\ 0 & I \end{pmatrix}$$
$$\cdot\begin{pmatrix} I & \begin{matrix} 0 & s_{12} & & & \\ s_{12} & 0 & & & \\ & & 0 & & \\ & & & \ddots & \\ & & & & 0 \end{matrix} \\ 0 & I \end{pmatrix}\cdot\cdots\cdot\begin{pmatrix} I & \begin{matrix} 0 & & & \\ & \ddots & & \\ & & 0 & \\ & & & 0 & s_{r-1,r} \\ & & & s_{r-1,r} & 0 \end{matrix} \\ 0 & I \end{pmatrix},$$

其中

$$S=\begin{pmatrix} s_{11} & s_{12} & \cdots & s_{1r} \\ s_{12} & s_{22} & \cdots & s_{2r} \\ \cdots & & \cdots & \\ s_{1r} & s_{2r} & \cdots & s_{rr} \end{pmatrix}，2r=n，形如\begin{pmatrix} I & \begin{matrix} 0 & & & & & \\ & \ddots & & & & \\ & & 0 & & & \\ & & & s_{ii} & & \\ & & & & 0 & \\ & & & & & \ddots \\ & & & & & & 0 \end{matrix} \\ 0 & I \end{pmatrix}$$

的元素显然为辛平延，其中$s_{ii}\neq 0$。如果$s_{ii}=0$，则为单位阵。

若T为辛平延，$V\in Sp_n(F)$，那么不难验证VTV^{-1}仍是辛平延。考虑下面等式

$$\begin{pmatrix} A & 0 \\ 0 & A^{-1\prime} \end{pmatrix}\begin{pmatrix} I^{(2)} & I \\ 0 & I^{(2)} \end{pmatrix}\begin{pmatrix} A & 0 \\ 0 & A^{-1\prime} \end{pmatrix}^{-1}$$

$$=\begin{pmatrix} I^{(2)} & AA' \\ 0 & I^{(2)} \end{pmatrix}=\begin{pmatrix} I^{(2)} & \begin{matrix} 1+\lambda^2 & \lambda \\ \lambda & 1 \end{matrix} \\ 0 & I^{(2)} \end{pmatrix},$$

其中$A=\begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix}$。

再计算

$$\begin{pmatrix} I^{(r)} & \begin{matrix} 1+\lambda^2 & \lambda & & \\ \lambda & 1 & & \\ & & 0 & \\ & & & \ddots \ 0 \end{matrix} \\ 0 & I^{(r)} \end{pmatrix}\cdot\begin{pmatrix} I^{(r)} & \begin{matrix} -(1+\lambda^2) & 0 & & \\ 0 & 0 & & \\ & & 0 & \\ & & & \ddots \ 0 \end{matrix} \\ 0 & I^{(r)} \end{pmatrix}$$

$$\cdot\begin{pmatrix} I^{(r)} & \begin{matrix} 0 & 0 & & \\ 0 & -1 & & \\ & & 0 & \\ & & & \ddots \ 0 \end{matrix} \\ 0 & I^{(r)} \end{pmatrix}=\begin{pmatrix} I^{(r)} & \begin{matrix} 0 & \lambda & & \\ \lambda & 0 & & \\ & & 0 & \\ & & & \ddots \ 0 \end{matrix} \\ 0 & I^{(r)} \end{pmatrix},$$

得到$\begin{pmatrix} I^{(r)} & S \\ 0 & I^{(r)} \end{pmatrix}$是平延的乘积。同样可证$\begin{pmatrix} I^{(r)} & 0 \\ T & I^{(r)} \end{pmatrix}$也是平延的乘积。

（2）对于$\begin{pmatrix} A & \\ & A'^{-1} \end{pmatrix}$，其中$A\in GL_r(F)$，先将$A$表成$A=\prod\limits_{i\neq j} T_{ij}(\lambda_{ij})\cdot D(d)$，其中$D(d)=\begin{pmatrix} 1 & & & \\ & 1 & & \\ & & \ddots & \\ & & & 1 & \\ & & & & d \end{pmatrix}$。于是

$$\begin{pmatrix} A & \\ & A'^{-1} \end{pmatrix} = \prod_{i \neq j} \begin{pmatrix} T_{ij}(\lambda_{ij}) & \\ & (T_{ij}(\lambda_{ij})')^{-1} \end{pmatrix} \begin{pmatrix} D(d) & \\ & D(d^{-1}) \end{pmatrix}。$$

要证明$\begin{pmatrix} A & \\ & A'^{-1} \end{pmatrix}$由平延生成，只要证明上式右端的每个因子由平延生成就行了。这可由下面的等式得出：

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \qquad (5\text{-}16)$$

$$\begin{pmatrix} d & 0 \\ 0 & d^{-1} \end{pmatrix} = \begin{pmatrix} 1 & -d \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ d^{-1} & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ d & 1 \end{pmatrix} \qquad (5\text{-}17)$$

$$\begin{pmatrix} 1 & & & \\ & 0 & & 1 \\ & & 1 & \\ & -1 & & 0 \end{pmatrix} \begin{pmatrix} 1 & \lambda & & \\ 0 & 1 & & \\ & & 1 & 0 \\ & & -\lambda & 1 \end{pmatrix} \begin{pmatrix} 1 & & & \\ & 0 & & -1 \\ & & 1 & \\ & 1 & & 0 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & & 0 & -\lambda \\ & 1 & -\lambda & 0 \\ & & 1 & \\ & & & 1 \end{pmatrix} \qquad (5\text{-}18)$$

（3）类型Ⅲ的阵利用式（5-16）可表成平延的乘积。

5.4.4 射影辛群的单性

已知辛群的中心$C(Sp_n(F))=\{I,-I\}$，简记为$C=\{I,-I\}$。辛群$Sp_n(F)$对它中心C的商群$Sp_n(F)/C$称为**射影辛群**，用$PSp_n(F)$表示，即$PSp_n(F)=Sp_n(F)/C$。这节的主要内容是证明，除某些特殊情形外，$PSp_n(F)$是单群。

定理5.4.7 若$\mathfrak{N}$是辛群$Sp_n(F)$的非中心的正规子群，那么$\mathfrak{N}=Sp_n(F)$，除$r=1$，$|F|=2$或3和$r=2$，$|F|=2$外，其中$2r=n$。

由此定理立即可得下面的系。

系5.4.6 射影辛群$PSp_n(F)$是单群，除$r=1$，$|F|=2$

或 3 和 $r=2$，$|F|=2$。

为了证明定理5.4.7，需要几个引理。

引理5.4.1 在定理 5.4.7 的假设下，若$\mathfrak{N}$包有一个辛平延，则$\mathfrak{N}=Sp_n(F)$。

证明 设辛平延$T=I+\lambda Bv'v\in\mathfrak{N}$，其中$\lambda\in F^*$，$v\neq 0$。由于任何二个非零向量在辛群之下可迁，因此存在$T_1\in Sp_n(F)$，使得$vT_1=(\underbrace{0,\cdots,0}_{r=\frac{n}{2}},1,\underbrace{0,\cdots,0}_{r-1})$，

$$T_1^{-1}TT_1=\begin{pmatrix} I^{(r)} & \begin{matrix}\lambda & & \\ & 0 & \\ & & \ddots \\ & & & 0\end{matrix} \\ & I^{(r)} \end{pmatrix}\in\mathfrak{N}。$$

令

$$\mathfrak{M}=\left\{\begin{pmatrix} a & & b & \\ & I^{(r-1)} & & 0^{(r-1)} \\ c & & d & \\ & 0^{(r-1)} & & I^{(r-1)} \end{pmatrix}\middle| ad-bc=1\right\},$$

易见$\mathfrak{M}\cong SL_2(F)\cong Sp_2(F)$，$\mathfrak{N}\cap\mathfrak{M}\lhd\mathfrak{M}$。由于

$$\mathfrak{N}\cap\mathfrak{M}\ni\begin{pmatrix} 1 & & \lambda & \\ & I^{(r-1)} & & \\ & & 1 & \\ & & & I^{(r-1)} \end{pmatrix},$$

根据引理5.1.1，$\mathfrak{N}\cap\mathfrak{M}$包有$\begin{pmatrix} 1 & & \mu & \\ & I^{(r-1)} & & 0^{(r-1)} \\ & & 1 & \\ & & & I^{(r-1)} \end{pmatrix}$，对任何$\mu\in F^*$，考虑

$$\begin{pmatrix} 0 & I^{(r)} \\ -I^{(r)} & 0 \end{pmatrix}\begin{pmatrix} 1 & & \mu & \\ & I^{(r-1)} & & 0^{(r-1)} \\ & & 1 & \\ & 0 & & I^{(r-1)} \end{pmatrix}\begin{pmatrix} 0 & I^{(r)} \\ -I^{(r)} & 0 \end{pmatrix}^{-1}$$

$$=\begin{pmatrix} I^{(r)} & & & 0 \\ -\mu & & & \\ & 0 & & \\ & & \ddots & I^{(r)} \\ & & & 0 \end{pmatrix},$$

根据定理5.4.3的（3），得到本引理。

引理5.4.2 $\mathfrak{N}$满足定理5.4.7的假设，则$\mathfrak{N}$必包有一个辛平延。

证明 由于$\mathfrak{N}$是辛群$Sp_n(F)$非中心的正规子群，则$\mathfrak{N}$必包有一个非中心元素T和存在一个辛平延$T_1=I+\lambda B\boldsymbol{v}'\boldsymbol{v}$，使得$T_2=T_1^{-1}T^{-1}T_1T\neq I$，和$T_2\in\mathfrak{N}$。将$T_1$代入$T_2$，得到

$$T_2=(I-\lambda B\boldsymbol{v}'\boldsymbol{v})(I+\lambda B(\boldsymbol{v}T)'(\boldsymbol{v}T))。$$

下面分两种情况讨论：

（a）$\boldsymbol{v}$与$\boldsymbol{v}T$线性相关。

设$\boldsymbol{v}T=\alpha\boldsymbol{v}$，$\alpha\in F^*$。则

$$\begin{aligned}T_2&=(I-\lambda B\boldsymbol{v}'\boldsymbol{v})(I+\lambda\alpha^2B\boldsymbol{v}'\boldsymbol{v})\\&=I-\lambda B\boldsymbol{v}'\boldsymbol{v}+\lambda\alpha^2B\boldsymbol{v}'\boldsymbol{v}\\&=I+(\lambda\alpha^2-\lambda)B\boldsymbol{v}'\boldsymbol{v}。\end{aligned}$$

如果$\lambda\alpha^2-\lambda\neq0$，则$T_2$是辛平延，而且$T_2\in\mathfrak{N}$。如果$\lambda\alpha^2-\lambda=0$，这与$T_2\neq I$矛盾。因此，对情形（a），$\mathfrak{N}$确包有一个辛平延。

（b）$\boldsymbol{v}$与$\boldsymbol{v}T$线性无关和$n\geqslant4$。（因为$n=2$时，$Sp_2(F)=SL_2(F)$。）再区分二种情形讨论：

（i）$\begin{pmatrix}\boldsymbol{v}\\ \boldsymbol{v}T\end{pmatrix}b\begin{pmatrix}\boldsymbol{v}\\ \boldsymbol{v}T\end{pmatrix}'=\begin{pmatrix}0&0\\0&0\end{pmatrix}$，即$\begin{pmatrix}\boldsymbol{v}\\ \boldsymbol{v}T\end{pmatrix}$是2维全迷向子空间，存在$T_3\in Sp_n(F)$，使得

$$\begin{pmatrix} v \\ vT \end{pmatrix} T_3 = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \end{pmatrix}。$$

令$T_4 = T_3^{-1} T_2 T_3$，则

$$T_4 = T_3^{-1}(I - \lambda B v' v)(I + \lambda B (vT)'(vT)) T_3$$

$$= \begin{pmatrix} I^{(r)} & & & & \\ \lambda & & & & \\ & 0 & & & I^{(r)} \\ & & \ddots & & \\ & & & 0 & \end{pmatrix} \begin{pmatrix} I^{(r)} & & & & \\ 0 & & & & \\ -\lambda & & & & \\ & 0 & & & I^{(r)} \\ & & \ddots & & \\ & & & 0 & \end{pmatrix}$$

$$= \begin{pmatrix} I^{(r)} & & & & \\ \lambda & & & & \\ -\lambda & & & & \\ & 0 & & & I^{(r)} \\ & & \ddots & & \\ & & & 0 & \end{pmatrix} \in \mathfrak{N}。$$

T_4本身不是平延，但可利用T_4造出一个包在$\mathfrak{N}$中的平延。考虑等式

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \lambda & \\ & -\lambda \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}' = \begin{pmatrix} 0 & -\lambda \\ -\lambda & -\lambda \end{pmatrix},$$

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 0 & -\lambda \\ -\lambda & -\lambda \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}' = \begin{pmatrix} & \lambda \\ \lambda & -\lambda \end{pmatrix},$$

可得

$$T_5 = \begin{pmatrix} I^{(r)} & & & & 0 \\ 0 & -\lambda & & & \\ -\lambda & -\lambda & & & \\ & & 0 & & I^{(r)} \\ & & & \ddots & \\ & & & & 0 \end{pmatrix} \in \mathfrak{N},$$

和

$$T_6=\begin{pmatrix} I^{(r)} & & & 0 \\ 0 & \lambda & & \\ \lambda & -\lambda & & \\ & & 0 & I^{(r)} \\ & & \ddots & \\ & & & 0 \end{pmatrix}\in\mathfrak{N}。$$

注意，这里用到$n\geqslant 4$。而对$n=2$时，已有$SL_2(F)=Sp_2(F)$。

$$T_5\cdot T_6=\begin{pmatrix} I^{(r)} & & & 0 \\ 0 & 0 & & \\ 0 & -2\lambda & & \\ & & 0 & I^{(r)} \\ & & \ddots & \\ & & & 0 \end{pmatrix}\in\mathfrak{N}。$$

如果域的特征$\neq 2$，则$T_5\cdot T_6$是$\mathfrak{N}$中的一个平延。引理得证。如果域的特征是2，取$A=\begin{pmatrix} a & \\ & a^{-1}\end{pmatrix}$，$a^2\neq 1$，这在$|F|>2$时总可取到。考虑等式

$$\begin{pmatrix} a^{-1} & 0 \\ 0 & a\end{pmatrix}\begin{pmatrix} 0 & -\lambda \\ -\lambda & -\lambda\end{pmatrix}\begin{pmatrix} a^{-1} & 0 \\ 0 & a\end{pmatrix}=\begin{pmatrix} 0 & -\lambda \\ -\lambda & -\lambda a^2\end{pmatrix},$$

可得

$$T_7=\begin{pmatrix} I^{(r)} & & & 0 \\ 0 & -\lambda & & \\ -\lambda & -\lambda a^2 & & \\ & & 0 & I^{(r)} \\ & & \ddots & \\ & & & 0 \end{pmatrix}\in\mathfrak{N},$$

$$T_8=\begin{pmatrix} I^{(r)} & 0 \\ \begin{matrix} 0 & -\lambda & & \\ -\lambda & -\lambda a^2 & & \\ & & 0 & \\ & & & \ddots & \\ & & & & 0 \end{matrix} & I^{(r)} \end{pmatrix}\begin{pmatrix} I^{(r)} & 0 \\ \begin{matrix} 0 & \lambda & & \\ \lambda & -\lambda & & \\ & & 0 & \\ & & & \ddots & \\ & & & & 0 \end{matrix} & I^{(r)} \end{pmatrix}$$

$$=\begin{pmatrix} I^{(r)} & \\ \begin{matrix} 0 & 0 & & \\ 0 & -\lambda(a^2+1) & & \\ & & 0 & \\ & & & \ddots & \\ & & & & 0 \end{matrix} & I^{(r)} \end{pmatrix}\in\mathfrak{N}。$$

由于$a^2\neq 1$，T_8是$\mathfrak{N}$中的一个平延。如果$|F|=2$，考虑$n\geqslant 6$的情形，为书写简单起见，不妨设$n=6$。T_4，T_6重新写出为

$$T_4=\begin{pmatrix} I^{(3)} & 0 \\ \begin{matrix} 1 & & \\ & 1 & \\ & & 0 \end{matrix} & I^{(3)} \end{pmatrix},\quad T_6=\begin{pmatrix} I^{(3)} & 0 \\ \begin{matrix} 0 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 0 \end{matrix} & I^{(3)} \end{pmatrix}。$$

考虑

$$T_9=\begin{pmatrix} \begin{matrix} & & 1 \\ & 1 & \\ 1 & & \end{matrix} & 0 \\ 0 & \begin{matrix} & & 1 \\ & 1 & \\ 1 & & \end{matrix} \end{pmatrix} T_4 \begin{pmatrix} \begin{matrix} & & 1 \\ & 1 & \\ 1 & & \end{matrix} & 0 \\ 0 & \begin{matrix} & & 1 \\ & 1 & \\ 1 & & \end{matrix} \end{pmatrix}^{-1}$$

$$=\begin{pmatrix} I^{(3)} & 0 \\ \begin{matrix} 0 & & \\ & 1 & \\ & & 1 \end{matrix} & I^{(3)} \end{pmatrix}\in\mathfrak{N},$$

$$T_{10}=\begin{pmatrix} I^{(3)} & 0 \\ \begin{matrix} 0 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 0 \end{matrix} & I^{(3)} \end{pmatrix} T_9 \begin{pmatrix} I^{(3)} & 0 \\ \begin{matrix} 0 & 1 & \\ 1 & 1 & \\ & 0 & \end{matrix} & I^{(3)} \end{pmatrix}^{-1}$$

$$=\begin{pmatrix} I^{(3)} & \\ \begin{matrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{matrix} & I^{(3)} \end{pmatrix} \in \mathfrak{N},$$

$$T_{11}=\begin{pmatrix} \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}'^{-1} & 0 \\ 0 & \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix} \end{pmatrix} T_{10} \begin{pmatrix} \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}'^{-1} & 0 \\ 0 & \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix} \end{pmatrix}^{-1}$$

$$=\begin{pmatrix} I^{(3)} & 0 \\ I^{(3)} & I^{(3)} \end{pmatrix} \in \mathfrak{N},$$

$$T_{12}=T_{11}\cdot T_9=\begin{pmatrix} I^{(3)} & 0 \\ \begin{matrix} 1 & & \\ & 0 & \\ & & 0 \end{matrix} & I^{(3)} \end{pmatrix} \in \mathfrak{N},$$

T_{12}是$\mathfrak{N}$中的一个平延。

(ii) $$\begin{pmatrix} v \\ vT \end{pmatrix} B \begin{pmatrix} v \\ vT \end{pmatrix}' = \begin{pmatrix} 0 & a \\ -a & a \end{pmatrix},\quad a \neq 0。$$

由于
$$\begin{pmatrix} 1 & 0 \cdots 0 & 0 \\ \underbrace{0 \cdots 0}_{r} & a & \underbrace{0 \cdots 0}_{r-1} \end{pmatrix} B \begin{pmatrix} 1 & 0 & \cdots & 0 \\ \underbrace{0 \cdots 0}_{r} & a & \underbrace{0 \cdots 0}_{r-1} \end{pmatrix}' = \begin{pmatrix} 0 & a \\ -a & 0 \end{pmatrix},$$

根据系5.4.3，存在$T_{13}\in Sp_{2r}(F)$，使得

$$\begin{pmatrix} 1 & 0 & \cdots & \cdots & 0 \\ \underbrace{0\cdots 0}_{r}, & a, & \underbrace{0,\cdots,0}_{r-1} \end{pmatrix} = \begin{pmatrix} v \\ vT \end{pmatrix} T_{13}。$$

重复前面的讨论，便得到引理。

引理5.4.3 $Sp_4(F_2) \cong S_6$，其中 S_6 是作用在6个文字上的完全对称群。

证明 设 V_4 是 F_2 上4维向量空间，$B = \begin{pmatrix} 0 & I^{(2)} \\ -I^{(2)} & 0 \end{pmatrix}$ 是 V_4 上非退化交错型。设 $\{\boldsymbol{x}_1, \boldsymbol{x}_2, \boldsymbol{y}_1, \boldsymbol{y}_2\}$ 是系5.3.1中所描述的 V_4 的基底，即 $\langle \boldsymbol{x}_1, \boldsymbol{y}_1\rangle \perp \langle \boldsymbol{x}_2, \boldsymbol{y}_2\rangle$ 和 $B(\boldsymbol{x}_1, \boldsymbol{y}_1) = B(\boldsymbol{x}_2, \boldsymbol{y}_2) = 1$，$B(\boldsymbol{y}_1, \boldsymbol{x}_1) = B(\boldsymbol{y}_2, \boldsymbol{x}_2) = -1$，$B(\boldsymbol{x}_i, \boldsymbol{x}_i) = B(\boldsymbol{y}_i, \boldsymbol{y}_i) = 0$，$i = 1, 2$。$V_4$中的15个非零向量为$\{\boldsymbol{x}_1, \boldsymbol{x}_2, \boldsymbol{x}_1+\boldsymbol{x}_2, \boldsymbol{y}_1, \boldsymbol{x}_1+\boldsymbol{y}_1, \boldsymbol{x}_2+\boldsymbol{y}_1, \boldsymbol{x}_1+\boldsymbol{x}_2+\boldsymbol{y}_1, \boldsymbol{y}_2, \boldsymbol{y}_1+\boldsymbol{y}_2, \boldsymbol{x}_1+\boldsymbol{y}_1+\boldsymbol{y}_2, \boldsymbol{x}_2+\boldsymbol{y}_1+\boldsymbol{y}_2, \boldsymbol{x}_1+\boldsymbol{x}_2+\boldsymbol{y}_1+\boldsymbol{y}_2, \boldsymbol{x}_1+\boldsymbol{y}_2, \boldsymbol{x}_2+\boldsymbol{y}_2, \boldsymbol{x}_1+\boldsymbol{x}_2+\boldsymbol{y}_2\}$，$V_4$中的一个子集合$C$，若它有5个元素，而且$C$中任何两个元素都不正交，则称$C$为一个**构形**。例如含有$\boldsymbol{x}_1$的构形有2个：

$$\{\boldsymbol{x}_1, \boldsymbol{y}_1, \boldsymbol{x}_1+\boldsymbol{y}_1+\boldsymbol{x}_2, \boldsymbol{x}_1+\boldsymbol{y}_1+\boldsymbol{y}_2, \\ \boldsymbol{x}_1+\boldsymbol{y}_1+\boldsymbol{x}_2+\boldsymbol{y}_2\}$$

和

$$\{\boldsymbol{x}_1, \boldsymbol{x}_1+\boldsymbol{y}_1, \boldsymbol{y}_1+\boldsymbol{x}_2, \boldsymbol{y}_1+\boldsymbol{y}_2, \boldsymbol{y}_1+\boldsymbol{x}_2+\boldsymbol{y}_2\}。$$

而且没有别的构形含有$\boldsymbol{x}_1$。实际上，可以验证：对每个$\boldsymbol{x}(\neq 0) \in V_4$，$\boldsymbol{x}$属于2个且只有2个构形$C$和$C'$，而且作为集合$C \cap C' = \{\boldsymbol{x}\}$。若在$V_4$中有$j$个不同的构形，则$5j = 2\times 15$，于是$j = 6$，即$V_4$中只有6个不同的构形。令$\Gamma = \{C_1, C_2, \cdots, C_6\}$。若$\sigma \in Sp_4(V) = Sp_4(F_2)$，则$\sigma C$是$V_4$的构形当且仅当$C$是$V_4$的构形。于是$\sigma$诱导出集合$\Gamma$上的一个置换$\tilde{\sigma} \in S_6$，映射$\sigma \to \tilde{\sigma}$给出群$Sp_4(F_2)$到$S_6$的一个同态。进而，这个同态是单射的。因为若$\sigma \in Sp_4(F_2)$，$\sigma \neq 1$，则存在$\boldsymbol{x} \in V_4$，$\sigma\boldsymbol{x} \neq \boldsymbol{x}$。设$\boldsymbol{x}$属于构

形C和C'，那么σx不可能同时属于C和C'。设$\sigma x \notin C$，因此$\sigma C \neq C$，于是$\tilde{\sigma} \neq 1$，这表明$\sigma \to \tilde{\sigma}$是单射。由于$|S_6| = 6! = 720$，$|Sp_4(F_2)| = 720$[●]，于是$\sigma \to \tilde{\sigma}$是满射的。由此得到$Sp_4(F_2) \cong S_6$。

定理5.4.7的证明 根据引理5.4.1和5.4.2，只要再说明$Sp_4(F_2)$包有一个非中心的正规子群就够了。由引理5.4.3，$Sp_4(F_2) \cong S_6$，而由偶置换全体组成的S_6的子群A_6是S_6的非中心正规子群。定理得证。

系5.4.7 除$n=2$，$|F|=2$或3，和$n=4$，$|F|=2$，辛群等于它自己的换位子群，即

$$Sp_n(F) = [Sp_n(F),\ Sp_n(F)]。$$

§5.5 二次型和对称双线性型

在线性代数中，讨论了实数域和复数域上的二次型，并给出了它们的标准型。在这节，将讨论一般域上的二次型及与它密切相关的对称双线性型。本章以下各节都假设域F的特征$\neq 2$。

定义5.5.1 二次型Q是一个由向量空间V到基域F的映射，它满足下面的条件：

（1）$Q(ax) = a^2 Q(x)$，对任何$a \in F$，$x \in V$。

（2）$B(x,\ y) = Q(x+y) - Q(x) - Q(y)$是双线性型。

称B为二次型Q相伴的双线性型。显然，B是对称双线性型，而且，由于域特征$\neq 2$，有$Q(x) = \frac{1}{2}B(x,\ x)$，即二次型$Q$可由相伴的双线性型所决定。另一方面，若$B$是给定的对称双线性型，那么令$Q(x) = B(x,\ x)$，是一个二次型，与此二次型相伴的对称双线性型是$B_1(x,\ y) = 2B(x,\ y)$。因此，研究二次型等价于研究对称双线性型。与交错型的情况相同，希望能找到对称双线性型在合同变换下的标准型或完全不变量。这对于

● 有限域F_q上辛群$Sp_{2r}(F_q)$的阶为：$(q^{2r}-1)q^{2r-1}(q^{2r-2}-1)q^{2r-3}\cdots(q^2-1)\cdot q$。

复数域与实数域的情况已经解决了。但对于任意域，这是一个很不简单的问题。$B=0$ 是平凡情形，以下的讨论总假设 $B\neq 0$。

设 B 是 n 维向量空间 V 上的对称双线性型，$(e_1, \cdots, e_n)$ 是 V 的基底。称矩阵 $S=(B(e_i, e_j))$ 为 B 相对基底 $(e_1, \cdots, e_n)$ 的对称阵（或简称为阵）。若 $(f_1, \cdots, f_n)$ 是 V 的另一基底，B 相对 $(f_1, \cdots, f_n)$ 的阵为 $S_1=(B(f_i, f_j))$。设 $f_i=\sum_{j=1}^{n} p_{ij}e_j$，$i=1, \cdots, n$，则 $B(f_i, f_j)=B\left(\sum_l p_{il}e_l, \sum_t p_{jt}e_t\right)=\sum_{l,t} p_{il}B(e_l, e_t)p'_{tj}$。于是有

$$S_1=PSP',$$

即向量空间 V 上的对称双线性型 B，在不同基底之下的阵表示合同。因此，求对称双线性型的标准型问题等价于求对称阵在合同变换下的标准型问题。

定理5.5.1 设 B 是基域 F 上 n 维向量空间 V 上的非零的对称双线性型，那么在 V 中存在一个基底 $(e_1, \cdots, e_n)$，使得 B 相对此基底的对称阵 C 有形式

$$\begin{pmatrix} b_1 & & & & & \\ & b_2 & & & & \\ & & \ddots & & & \\ & & & b_r & & \\ & & & & 0 & \\ & & & & & \ddots & \\ & & & & & & 0 \end{pmatrix}^{●}, \tag{5-19}$$

其中 $b_i\neq 0$，$1\leqslant i\leqslant r$，$1\leqslant r\leqslant n$。

证明 先通过矩阵运算给出证明，然后用几何方法给出另一证明，使读者可从中进行比较。

（1）设与 B 相应的对称阵是

● 矩阵中未列出的元素均是 0 元素，以下同。

$$C_1=\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{12} & a_{22} & \cdots & a_{2n} \\ \vdots & & \ddots & \\ a_{1n} & & \cdots & a_{nn} \end{pmatrix}。$$

对 $n=\dim V$ 施归纳法证明定理。

（a） $n=1$，显然。

（b）假设 $\dim V=n-1$ 时定理成立。今证明 $\dim V=n$ 时定理成立。分三种情况讨论：

（i）设 $a_{11}\neq 0$，那么

$$\begin{pmatrix} 1 & & & \\ -a_{12}a_{11}^{-1} & 1 & & \\ \vdots & & \ddots & \\ -a_{1n}a_{11}^{-1} & & & 1 \end{pmatrix} C_1 \begin{pmatrix} 1 & & & \\ -a_{12}a_{11}^{-1} & 1 & & \\ \vdots & & \ddots & \\ -a_{1n}a_{11}^{-1} & & & 1 \end{pmatrix}'$$

$$=\begin{pmatrix} a_{11} & 0 & \cdots & 0 \\ 0 & b_{22} & \cdots & b_{2n} \\ \vdots & \vdots & \ddots & \\ 0 & b_{n2} & & b_{nn} \end{pmatrix}。$$

(ii) $a_{11}=0$，但存在某个 $a_{ii}\neq 0$，那么

$$i\text{行}\begin{pmatrix} 0 & & & & 1 & & & \\ & 1 & & & & & & \\ & & 1 & & & & & \\ & & & \ddots & & & & \\ & & & & 1 & & & \\ 1 & & & & & 0 & & \\ & & & & & & 1 & \\ & & & & & & & \ddots \\ & & & & & & & & 1 \end{pmatrix} C_1 \begin{pmatrix} 0 & & & & 1 & & & \\ & 1 & & & & & & \\ & & 1 & & & & & \\ & & & \ddots & & & & \\ & & & & 1 & & & \\ 1 & & & & & 0 & & \\ & & & & & & 1 & \\ & & & & & & & \ddots \\ & & & & & & & & 1 \end{pmatrix}'$$

$$=\begin{pmatrix} a_{ii} & b_{12} & \cdots & b_{1n} \\ b_{12} & b_{22} & & \vdots \\ \vdots & & \ddots & \vdots \\ b_{1n} & \cdots & & b_{nn} \end{pmatrix},$$

化为情形（i）。

(iii) $a_{ii}=0$，$i=1, 2, \cdots, n$。如果 $B=0$，定理显然成立。如果 $B\neq 0$，必存在 $a_{ij}\neq 0$，$i\neq j$。不失一般性，设

$a_{12}\neq 0$。

$$\begin{pmatrix}1 & \frac{1}{2} & & & \\ & 1 & & & \\ & & 1 & & \\ & & & \ddots & \\ & & & & 1\end{pmatrix}\begin{pmatrix}0 & a_{12} & & \cdots & a_{1n} \\ a_{12} & 0 & a_{23} & \cdots & a_{2n} \\ a_{13} & a_{23} & 0 & & \vdots \\ \vdots & \vdots & & \ddots & a_{n-1,n} \\ a_{1n} & a_{2n} & & a_{n-1,n} & 0\end{pmatrix}\begin{pmatrix}1 & \frac{1}{2} & & \\ & 1 & & \\ & & \ddots & \\ & & & 1\end{pmatrix}'$$

$$=\begin{pmatrix}a_{12} & b_{12} & \cdots & b_{1n} \\ b_{12} & b_{22} & \cdots & b_{2n} \\ \vdots & & \ddots & \vdots \\ b_{1n} & & & b_{nn}\end{pmatrix},$$

化为情形（ii）。

综合上述，再根据归纳法假设，便得到定理。

（2）几何方法的证明

因为$B\neq 0$，故必存在$\boldsymbol{u}\in V$，使得$B(\boldsymbol{u}_1\boldsymbol{u})\neq 0$。否则的话，$0=B(\boldsymbol{u}+\boldsymbol{v},\ \boldsymbol{u}+\boldsymbol{v})=2B(\boldsymbol{u},\ \boldsymbol{v})$，于是对任何$\boldsymbol{u}$和$\boldsymbol{v}$都有$B(\boldsymbol{u},\ \boldsymbol{v})=0$，这与$B\neq 0$矛盾。令$\boldsymbol{u}=\boldsymbol{u}_1$，$V_1=F\boldsymbol{u}_1$，显然$B$限制在$V_1$上是非退化的，有$V_1\cap V_1^{\perp}=\{\boldsymbol{0}\}$。设$b_1=B(\boldsymbol{u}_1,\ \boldsymbol{u}_1)$，对于$\boldsymbol{x}\in V$，令$\boldsymbol{y}=\boldsymbol{x}-b_1^{-1}B(\boldsymbol{x},\ \boldsymbol{u}_1)\boldsymbol{u}_1$，计算

$$B(\boldsymbol{y},\ \boldsymbol{u}_1)=B(\boldsymbol{x},\ \boldsymbol{u}_1)-b_1^{-1}B(\boldsymbol{x},\ \boldsymbol{u}_1)B(\boldsymbol{u}_1,\ \boldsymbol{u}_1)=0,$$

由此得出$\boldsymbol{y}\in V_1^{\perp}$，$\boldsymbol{x}=\boldsymbol{y}+b_1^{-1}B(\boldsymbol{x},\ \boldsymbol{u}_1)\boldsymbol{u}_1$，$V=V_1\oplus V_1^{\perp}$。如果$B|_{V_1^{\perp}}=0$，那么取$r=1$，及$V_1^{\perp}$的基$(\boldsymbol{z}_1,\ \cdots,\ \boldsymbol{z}_{n-1})$，则在$V$的基$(\boldsymbol{u}_1,\ \boldsymbol{z}_1,\ \cdots,\ \boldsymbol{z}_{n-1})$之下，$B$的阵表示形如式(5-19)。如果$B|_{V_1^{\perp}}\neq 0$，则有$\boldsymbol{u}_2\in V_1^{\perp}$，使得$B(\boldsymbol{u}_2,\ \boldsymbol{u}_2)=b_2\neq 0$。重复上述步骤，有限步后，可得到定理。

定义5.5.2 设B是V上的对称双线性型和$(\boldsymbol{u}_1,\ \cdots,\ \boldsymbol{u}_n)$是$V$的基底，而且对所有的$i\neq j$都有$B(\boldsymbol{u}_i,\ \boldsymbol{u}_j)=0$，那么称$(\boldsymbol{u}_1,\cdots,\ \boldsymbol{u}_n)$是$V$相对$B$的正交基。

由定理5.5.1知，向量空间V相对任意给定的对称双线性型都存在正交基，但并没有正交基唯一的结果，用矩阵的语言即是，任何对称阵在合同变换下可化为对角型阵，但此对角阵也不能由

B唯一确定。我们希望得到对称矩阵在合同变换下的完全不变量，例如在基域是复数域时，其完全不变量就是矩阵的秩，基域是实数域时，其完全不变量是矩阵的秩和符号差。在复数域上，两个对称矩阵合同当且仅当它们有相同的秩；在实数域上，两个对称矩阵合同当且仅当它们有相同的秩和符号差。完全不变量的确定，很强地依赖于基域的算术性质。对于基域F是有理数域时，闵可夫斯基（Minkowski）和哈塞（Hasse）解决了这个问题。他们应用了代数中赋值论的工具。代数闭域的情形与复数域结果相同，实闭域情形与实数域相同。此外，有限域的情况也比较简单，由于篇幅的关系，不在这里讨论了。有兴趣的读者可参阅参考文献〔6〕。

系5.5.1 设U是V的子空间，B是V上的对称双线性型。如果${}^B|_U$是非退化的，那么U的正交基可以扩充为V的正交基。

证明 ${}^B|_U$是U上的对称双线性型。由定理5.5.1，U有一正交基$(\boldsymbol{u}_1, \cdots, \boldsymbol{u}_r)$，$r=\dim U$，使得${}^B|_U$上的阵表示为

$$\begin{pmatrix} b_1 & & & \\ & b_2 & & \\ & & \ddots & \\ & & & b_r \end{pmatrix},$$

其中$b_i = B(\boldsymbol{u}_i, \boldsymbol{u}_i)$。由于${}^B|_U$是非退化的，则$b_i \neq 0$，$i=1$，2，$\cdots$，$r$，而且$U \cap U^{\perp} = \{\boldsymbol{0}\}$。设$\boldsymbol{x} \in V$，令

$$\boldsymbol{y} = \boldsymbol{x} - \sum_{i=1}^{r} B(\boldsymbol{x}, \boldsymbol{u}_i) b_i^{-1} \boldsymbol{u}_i,$$

计算

$$B(\boldsymbol{y}, \boldsymbol{u}_j) = B(\boldsymbol{x}, \boldsymbol{u}_j) - \sum_{i=1}^{r} B(\boldsymbol{x}, \boldsymbol{u}_i) b_i^{-1} B(\boldsymbol{u}_i, \boldsymbol{u}_j) = 0。$$

因此$\boldsymbol{y} \in U^{\perp}$，从而得到$V = U \oplus U^{\perp}$。下面采用定理5.5.1的证明方法，便得到此系。

系5.5.2 设B是向量空间V上的对称双线性型，它在V的基底$(\boldsymbol{u}_1, \cdots, \boldsymbol{u}_r, \boldsymbol{z}_1, \cdots, \boldsymbol{z}_{n-r})$有阵表示

$$\begin{pmatrix} b_1 & & & & & \\ & b_2 & & & & \\ & & \ddots & & & \\ & & & b_r & & \\ & & & & 0 & \\ & & & & & \ddots \\ & & & & & & 0 \end{pmatrix},\quad b_i \neq 0,\quad 1 \leqslant i \leqslant r,$$

那么 $V^{\perp} = \sum\limits_{i=1}^{n-r} F z_i$。

证明 设 $x \in V$，则 $\boldsymbol{x} \in V^{\perp}$ 当且仅当 $B(\boldsymbol{u}_i, \boldsymbol{x}) = 0$，$1 \leqslant i \leqslant r$ 和 $B(z_j, \boldsymbol{x}) = 0$，$1 \leqslant j \leqslant n-r$。设 $\boldsymbol{x} = \sum\limits_{i=1}^{r} a_i \boldsymbol{u}_i + \sum\limits_{j=1}^{n-r} b_j \boldsymbol{z}_j$，$B(\boldsymbol{u}_i, \boldsymbol{x}) = B\left(\boldsymbol{u}_i, \sum\limits_{i=1}^{r} a_i \boldsymbol{u}_i + \sum\limits_{j=1}^{n-r} b_j \boldsymbol{z}_j\right) = a_i b_i$。$B(\boldsymbol{u}_i, \boldsymbol{x}) = 0$ 当且仅当 $a_i = 0$，因为 $b_i \neq 0$。再考虑到 $B(\boldsymbol{z}_j, \boldsymbol{x}) = 0$，$1 \leqslant j \leqslant n-r$。因此 $\boldsymbol{x} \in V^{\perp}$ 当且仅当 $\boldsymbol{x} \in \sum\limits_{j=1}^{n-r} F \boldsymbol{z}_j$。

§5.6 正 交 群

5.6.1 定义

域 F 上的有限维向量空间 V 和它上面的非退化对称双线性型 B 被称为**正交空间**，用 (V, B) 表示。由于在域特征 $\neq 2$ 时，给定的二次型 Q 有相伴的对称双线性型 B，$B(\boldsymbol{x}, \boldsymbol{y}) = Q(\boldsymbol{x}+\boldsymbol{y}) - Q(\boldsymbol{x}) - Q(\boldsymbol{y})$，而且给定一个对称双线性型 B 有相伴的二次型 Q，$Q(\boldsymbol{x}) = \frac{1}{2} B(\boldsymbol{x}, \boldsymbol{x})$。因此正交空间也用 (V, Q) 表示。令 (V_1, Q_1)，(V_2, Q_2) 是二个正交空间，那么由 (V_1, Q_1) 到 (V_2, Q_2) 的一个**等距变换** η 是指 η 是 V_1 到 V_2 之上的可逆线性变换，而且对任何 $\boldsymbol{x} \in V_1$ 满足 $Q_2(\eta(\boldsymbol{x})) = Q_1(\boldsymbol{x})$。这时也称空间 V_1 和 V_2 是**等距的**。设 B_i 是与 Q_i 相伴的

对称双线性型，不难验证 $B_2(\eta(\boldsymbol{x}),\ \eta(\boldsymbol{y}))=B_1(\boldsymbol{x},\ \boldsymbol{y})$，对任何 $\boldsymbol{x},\ \boldsymbol{y}\in V_1$，如果存在由 $(V_1,\ Q_1)$ 到 $(V_2,\ Q_2)$ 的一个等距变换，则称二次型 Q_1 和 Q_2 是等价的，其相伴的对称双线性型 B_1 和 B_2 也称为等价的。

如果 Q 是向量空间 V 上非退化的二次型，则 V 到 V 之上的等距变换称为 V（或 $(V,\ Q)$）的**正交变换**。事实上，若 η 是 V 到 V 之中的线性变换，满足 $Q(\eta(\boldsymbol{x}))=Q(\boldsymbol{x})$，对所有 $\boldsymbol{x}\in V$，则 η 必是正交变换。因为 $Q(\eta(\boldsymbol{x}))=Q(\boldsymbol{x})$，则对 Q 的相伴对称双线性型 B，有 $B(\eta(\boldsymbol{x}),\ \eta(\boldsymbol{y}))=B(\boldsymbol{x},\ \boldsymbol{y})$，对所有 $\boldsymbol{x}$，$\boldsymbol{y}\in V$。于是若 $\eta(\boldsymbol{x})=0$，那么对所有 $\boldsymbol{y}\in V$，$B(\boldsymbol{x},\boldsymbol{y})=0$。因为 B 是非退化的，因此 $\boldsymbol{x}=0$，即 η 是一一变换。再考虑到 V 是有限维的，所以 η 是映上。这表明 η 是正交变换。V 的正交变换全体成群，用 $O(V,\ Q)$ 表示，称为 V 相对 Q 的**正交群**。$O(V,\ Q)$ 是 $GL(V)$ 的子群，

$$O(V,\ Q)=\{\eta\in GL(V)\,|\,Q(\eta(\boldsymbol{x}))=Q(\boldsymbol{x})\ \ \forall \boldsymbol{x}\in V\}。$$

设 $(\boldsymbol{e}_1,\ \cdots,\ \boldsymbol{e}_n)$ 是 V 的基底．V 上非退化对称双线性型 B 相对此基底的阵表示是 S，V 上可逆线性变换 η 相对此基底的阵表示是 T，那么 $\eta\in O(V,\ Q)$ 当且仅当 $TST'=S$。因为 $\eta\in O(V,\ Q)$ 当且仅当 $B(\eta(\boldsymbol{x}),\ \eta(\boldsymbol{y}))=B(\boldsymbol{x},\boldsymbol{y})$，$B(\eta(\boldsymbol{x}),\ \eta(\boldsymbol{y}))=B(\boldsymbol{x},\ \boldsymbol{y})$ 当且仅当 $B(\eta(\boldsymbol{e}_i),\ \eta(\boldsymbol{e}_j))=B(\boldsymbol{e}_i,\ \boldsymbol{e}_j)$，对于 $1\leqslant i,\ j\leqslant n$。$\eta(\boldsymbol{e}_i)=\sum\limits_{j=1}^{n} t_{ij}\boldsymbol{e}_j$，$(t_{ij})=T$。将 $\eta(\boldsymbol{e}_i)$ 代入上面等式，便得到 $S=TST'$。进而，计算行列式，$\det S=(\det T)^2\cdot\det S$。由于 B 是非退化的，$(\det S)^{-1}$ 存在，因此 $\det T=\pm 1$。如果 $\det T=1$，称 T 为**旋转**或**正常的**正交变换；如果 $\det T=-1$，称 T 为**非正常的**正交变换。由于同一线性变换虽然相对不同基底有不同的阵表示，但其阵表示的行列式的值是相同的。因此把线性变换在某一基底下的阵表示的行列式就定义为此

线性变换的行列式，于是有 $\det\eta=\det T$。令 $O^+(V, Q)=\{\eta\in O(V, Q)|\det\eta=1\}$，即 $O^+(V, Q)$ 是由$O(V,Q)$ 中的旋转组成的子群。不难看出，$O^+(V, Q)\lhd O(V, Q)$，和 $(O: O^+)=2$，这里$O=O(V,Q)$。

设 B_1 和 B_2 是两个非退化的对称双线性型，而且彼此合同，那么有群同构

$$O(V, Q_1)\cong O(V, Q_2),$$

其中 Q_i 是与 B_i 相伴的二次型。此证明与辛群的情况完全相同，请读者证明。由于这个结果，在研究正交群时，总是选取对角型的对称阵决定的对称双线性型来考虑。例如，在实数域上，如果二次型Q是定正的，那么可取 $S=I$。这时条件 $TST'=S$就是 $TT'=I$，这正是在线性代数中学习的实数域上正交阵的定义。

下面讨论在正交群中起重要作用的、称为对称的正交变换。设 $\boldsymbol{u}\in V$，满足 $Q(\boldsymbol{u})\neq 0$，那么它决定一个正交变换 $S_u: \boldsymbol{x}\to \boldsymbol{x}-\dfrac{B(\boldsymbol{x}, \boldsymbol{u})}{Q(\boldsymbol{u})}\boldsymbol{u}$，其中$B$是$Q$ 相伴的对称双线性型。由于 $\boldsymbol{x}\to \boldsymbol{x}$ 和 $\boldsymbol{x}\to B(\boldsymbol{x}, \boldsymbol{u})\boldsymbol{v}$ 对任何 $\boldsymbol{u}$，$\boldsymbol{v}$ 都是线性的，因此 S_u 是线性的。计算

$$\begin{aligned}Q(S_u(\boldsymbol{x}))&=Q\left(\boldsymbol{x}-\frac{B(\boldsymbol{x}, \boldsymbol{u})}{Q(\boldsymbol{u})}\boldsymbol{u}\right)\\&=Q(\boldsymbol{x})+\frac{B(\boldsymbol{x},\boldsymbol{u})^2}{Q(\boldsymbol{u})^2}Q(\boldsymbol{u})\\&\quad-\frac{B(\boldsymbol{x}, \boldsymbol{u})}{Q(\boldsymbol{u})}B(\boldsymbol{x}, \boldsymbol{u})=Q(\boldsymbol{x}),\end{aligned}$$

因此 S_u 确是正交变换，称 S_u 为 $\boldsymbol{u}$ 决定的**对称**。$S_u(\boldsymbol{u})=-\boldsymbol{u}$，和如果 $\boldsymbol{v}\perp\boldsymbol{u}$，即 $B(\boldsymbol{u},\boldsymbol{v})=0$，则 $S_u(\boldsymbol{v})=\boldsymbol{v}$。由于 $B(\boldsymbol{u}, \boldsymbol{u})\neq 0$，$S_u|_{F\boldsymbol{u}}$ 是非退化的，因此$V=F\boldsymbol{u}\oplus F\boldsymbol{u}^\perp$。现在，可以给出 S_u 的几何描述：它在子空间 $F\boldsymbol{u}^\perp$上是恒等变换，而将$\boldsymbol{u}$变到$-\boldsymbol{u}$。如果取 F 为实数域，B_1 为通常内积，即 $B_1(\boldsymbol{x}, \boldsymbol{y})=\sum\limits_{i=1}^{3}x_iy_i$，其中

$x=\sum_{i=1}^{3}x_ie_i$，$y=\sum_{i=1}^{3}y_ie_i$。令$Q(x)=(x,x)$，与 Q 相伴的对称双线性型$B(x,y)=2(x,y)$。那么 $S_u(x)=x-\frac{2(x,u)}{(u,u)}u=x-2\left(x,\frac{u}{\|u\|}\right)\frac{u}{\|u\|}$，其中 $(u,u)=\|u\|^2$。$S_u(x)$ 是 x 对于过原点与 u 垂直的平面W的镜像，见图 5-1。取 $u_1=u$ 为 Fu的基底，$(u_2,\cdots,u_n)$ 为 $Fu^{\perp}$ 的正交基底，那么 S_u 相对正交基 $(u_1,u_2,\cdots,u_n)$ 的阵表示是

$$\begin{pmatrix}-1&&&&\\&1&&&\\&&1&&\\&&&\ddots&\\&&&&1\end{pmatrix},$$

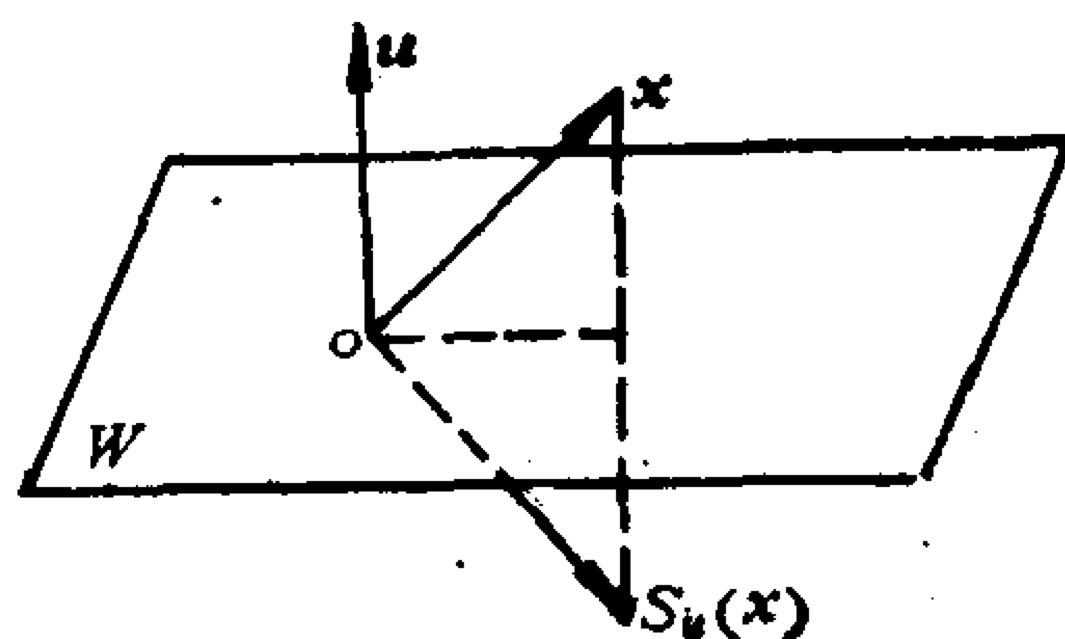


图 5-1

$\det S_u=-1$，$S_u^2=1$。如果 η 是任意一个正交变换，那么 $\eta S_u\eta^{-1}=S_{\eta(u)}$。这只要通过具体计算就可得到：

$$\eta S_u\eta^{-1}(x)=\eta\left(\eta^{-1}(x)-\frac{B(\eta^{-1}(x),u)}{Q(u)}u\right)$$

$$=x-\frac{B(\eta^{-1}(x),u)}{Q(u)}\eta(u)$$

$$=x-\frac{B(x,\eta(u))}{Q(\eta(u))}\eta(u)=S_{\eta(u)}(x)。$$

V 的两个子空间 U_1 和 U_2 正交，常用 $U_1\perp U_2$ 表示，是指 $B(x,y)=0$，对所有 $x\in U_1$，$y\in U_2$。空间V是子空间 U_1，$\cdots$，U_r 的一个**正交直和分解**，如果有（1）$V=U_1\oplus\cdots\oplus U_r$ 和（2）对所有 $i\neq j$，有 $U_i\perp U_j$。这时可将V表成

$$V=U_1\perp U_2\perp\cdots\perp U_r。$$

对于 $x\in V$，可将 x表成 $x=\sum_{i=1}^{r}x_i$，$x_i\in U_r$。那么

$$Q(x)=Q\left(\sum_{i=1}^{r} x_i\right)=\sum_{i=1}^{r} Q(x_i).$$

由于Q是非退化的，易见$Q|_{U_i}$仍然是非退化的。注意，一般说来，如果Q在空间V上是非退化的，将Q限制在任一子空间U上，不一定是非退化的。

对于$x\in V$，若$x\neq 0$，而且$Q(x)=0$，则称x为**迷向向量**。V的子空间U称为**迷向的**，如果U包有一个迷向向量；U是**全迷向子空间**，如果$Q|_U=0$，即$Q(u)=0$，对所有$u\in U$。显然，U是全迷向的当且仅当$U\subset U^{\perp}$。V的非退化的、迷向的二维子空间称为**双曲平面**。

定理5.6.1 （1）设V是二维向量空间，Q是V上的二次型，那末下列叙述是等价的：

（i）V是一个双曲平面。

(ii) V有基底$(u,\ v)$，使得

$$B(u,u)=B(v,v)=0,\quad B(u,v)=B(v,u)=1,$$

称具此性质的基底为**双曲对**。

(iii) $\det B=-1\cdot a^2$，对某个$a\in F^*$。

（2）对任何二个双曲平面V_1和V_2，都存在等距变换η，使得$\eta V_1=V_2$。

（3）任何双曲平面都包有2个且只有2个一维全迷向子空间。

（4）双曲平面V的旋转群$O^+(F,V)$同构于域F的非零元全体F^*的乘法群；V的每个非正常正交变换是一个对称。

证明 （1）（i）⇒(ii)：因为V是双曲平面，它包有迷向向量u，$u\neq 0$和$B(u,u)=0$。由于B是非退化的，则存在$v\in V$使得$B(u,\ v_1)=b\neq 0$。令$v_2=b^{-1}v_1$，那么$B(u,v_2)=1$。显然u与v_2是线性无关的。令

$$v=v_2-Q(v_2)u,$$

$$B(v,v)=B(v_2-Q(v_2)u,\ v_2-Q(v_2)u)$$

$$=2Q(v_2)-2Q(v_2)=0.$$

$$B(\boldsymbol{v}, \boldsymbol{u}) = B(\boldsymbol{v}_2 - Q(\boldsymbol{v}_2)\boldsymbol{u}, \boldsymbol{u})$$
$$= 1 = B(\boldsymbol{u}, \boldsymbol{v})。$$

(ii)⇒(iii) 由（i），B相对任何基底的阵表示为

$$C = P\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} P'$$

其中$P \in GL_2(F)$，$\det P = a \in F^*$，于是$\det C = -1 \cdot a^2$。

(iii)⇒(i) 由于B的阵表示是可逆阵，因此B是非退化的。由定理5.5.1得知，存在正交基（$\boldsymbol{u}, \boldsymbol{v}$），使得$B$的阵表示$C$有对角型，$C = \begin{pmatrix} b_1 & 0 \\ 0 & b_2 \end{pmatrix}$，$b_i \neq 0$，$i = 1, 2$。由（iii），$\det C = -a^2 = b_1 b_2$，对某个$a \in F^*$，令$\boldsymbol{u}_1 = a\boldsymbol{u} + b_1\boldsymbol{v}$，计算$B(\boldsymbol{u}_1, \boldsymbol{u}_1) = B(a\boldsymbol{u} + b_1\boldsymbol{v}, a\boldsymbol{u} + b_1\boldsymbol{v}) = a^2 b_1 + b_1^2 b_2 = 0$。因此$\boldsymbol{u}$是$V$中的迷向向量。得到（i）。

（2）设双曲平面V_i有双曲对（$\boldsymbol{u}_i$，$\boldsymbol{v}_i$），$i = 1, 2$。令映射η将V_1的任一元素$a\boldsymbol{u}_1 + b\boldsymbol{v}_1$映到$a\boldsymbol{u}_2 + b\boldsymbol{v}_2$，则$\eta$是$V_1$到$V_2$的等距变换。为此只要验证$Q(\eta(a\boldsymbol{u}_1 + b\boldsymbol{v}_1)) = Q(a\boldsymbol{u}_1 + b\boldsymbol{v}_1)$。

$$Q(\eta(a\boldsymbol{u}_1 + b\boldsymbol{v}_1)) = Q(a\boldsymbol{u}_2 + b\boldsymbol{v}_2)$$
$$= a^2 Q(\boldsymbol{u}_2) + b^2 Q(\boldsymbol{v}_2) + ab$$
$$= Q(a\boldsymbol{u}_1 + b\boldsymbol{v}_1)。$$

（3）设双曲平面V的双曲对为（$\boldsymbol{u}, \boldsymbol{v}$）。显然，$F\boldsymbol{u}$和$F\boldsymbol{v}$是两个不同的一维全迷向子空间。若向量$\boldsymbol{x} = a\boldsymbol{u} + b\boldsymbol{v}$，满足$Q(\boldsymbol{x}) = 0$，则有

$$0 = Q(\boldsymbol{x}) = ab。$$

因此，a与b之一必为0，即$\boldsymbol{x} \in F\boldsymbol{u}$或$\boldsymbol{x} \in F\boldsymbol{v}$。这表明$V$有且只有上面2个一维全迷向子空间。

（4）设$\eta \in O(V, F)$，（$\boldsymbol{u}, \boldsymbol{v}$）是$V$的双曲对，$\eta(\boldsymbol{u}) = a\boldsymbol{u} + b\boldsymbol{v}$。由$Q(\eta(\boldsymbol{u})) = Q(\boldsymbol{u}) = 0$，得到$ab = 0$。若$a = 0$，$\eta(\boldsymbol{u}) = b\boldsymbol{v}$。由此有$\eta(\boldsymbol{v}) \in F\boldsymbol{u}$。设$\eta(\boldsymbol{v}) = a'\boldsymbol{u}$。由$B(\eta(\boldsymbol{u}), \eta(\boldsymbol{v})) = B(\boldsymbol{u}, \boldsymbol{v}) = 1$，有$a'b = 1$。于是$\eta$相对基（$\boldsymbol{u}, \boldsymbol{v}$）的

阵表示为

$$\begin{pmatrix} 0 & b^{-1} \\ b & 0 \end{pmatrix},$$

$\det\eta=-1$，即η是非正常的。$\eta(u+bv)=u+bv$，$\eta(u-bv)=-(u-bv)$。进而，$B(u+bv,\ u-bv)=0$，得出$(u+bv,\ u-bv)$是正交基，$\eta=S_{u-bv}$是一个对称。若$b=0$，$\eta(u)=au$。由此有$\eta(v)\in Fv$。设$\eta(v)=b_1v$。由$B(\eta(u),\eta(v))=B(u,\ v)$，得出$ab_1=1$。$\eta$相对基$(u,\ v)$的阵表示为

$$\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix},$$

$\det\eta=1$，$\eta\in O^+(V,\ F)$。再根据上面的讨论，得到$\eta\in O^+(V,F)$当且仅当$b=0$，$b=0$当且仅当η有阵表示

$$\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix},\quad a\neq 0。$$

映射$\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}\to a$给出$O^+(V,\ Q)$到$F^*=F\setminus\{0\}$的同构。

5.6.2 消去定理

二次型的分类对研究正交群有着十分重要的意义，而由维特(Witt)给出的消去定理对二次型的分类问题起着本质性的作用。这节主要证明消去定理。特约定，在本章以下各节，V总是表示特征$\neq 2$的基域F上的n维向量空间。

定理5.6.2 设Q是向量空间V上的非退化的二次型，U_1和U_2是V的非退化的子空间，而且是等距的，那么$U_1^{\perp}$和$U_2^{\perp}$也是等距的。

证明 用符号"$\approx$"表示等距。由定理假设，有

$$V=U_1\oplus U_1^{\perp}=U_2\oplus U_2^{\perp}$$

和

$$U_1\approx U_2。$$

今要证明$U_1^{\perp}\approx U_2^{\perp}$。对$\dim U_1(=\dim U_2)$采取归纳法来证明定理。

假设$\dim U_i=1$，和$U_i=F\boldsymbol{u}_i$，$i=1,2$。由于$Q|_{U_i}$是非退化的，有$Q(\boldsymbol{u}_i)\neq 0$。由于$F\boldsymbol{u}_1\approx F\boldsymbol{u}_2$，不失一般性，假设$Q(\boldsymbol{u}_1)=Q(\boldsymbol{u}_2)$。于是$Q(\boldsymbol{u}_1\pm\boldsymbol{u}_2)=2Q(\boldsymbol{u}_1)\pm B(\boldsymbol{u}_1,\boldsymbol{u}_2)$。由此有$Q(\boldsymbol{u}_1+\boldsymbol{u}_2)\neq 0$或者$Q(\boldsymbol{u}_1-\boldsymbol{u}_2)\neq 0$。否则的话，$Q(\boldsymbol{u}_1)=0$。假设$Q(\boldsymbol{u}_1+\boldsymbol{u}_2)\neq 0$，考虑$B(\boldsymbol{u}_1+\boldsymbol{u}_2,\ \boldsymbol{u}_1-\boldsymbol{u}_2)=0$，有$S_{u_1+u_2}(\boldsymbol{u}_1+\boldsymbol{u}_2)=-(\boldsymbol{u}_1+\boldsymbol{u}_2)$，$S_{u_1+u_2}(\boldsymbol{u}_1-\boldsymbol{u}_2)=\boldsymbol{u}_1-\boldsymbol{u}_2$，于是$S_{u_1+u_2}(\boldsymbol{u}_1)=-\boldsymbol{u}_2$，$S_{u_1+u_2}(F\boldsymbol{u}_1)=F\boldsymbol{u}_2$，$S_{u_1+u_2}(F\boldsymbol{u}_1^{\perp})=F\boldsymbol{u}_2^{\perp}$。得到$F\boldsymbol{u}_1^{\perp}\approx F\boldsymbol{u}_2^{\perp}$。对于$Q(\boldsymbol{u}_1-\boldsymbol{u}_2)\neq 0$的情况，作类似的讨论，可得到同样结果：$F\boldsymbol{u}_1^{\perp}\sim F\boldsymbol{u}_2^{\perp}$。

假设定理对于$\dim U_i<r$成立，可证明定理对于$\dim U_i=r$时也成立。由于$B|_{U_1}$是非退化的，那么存在$\boldsymbol{u}_1\in U_1$，使得$Q(\boldsymbol{u}_1)\neq 0$。由系5.5.1 U_1可分解为

$$U_1=F\boldsymbol{u}_1\perp W_1,$$

其中W_1是$F\boldsymbol{u}_1$在U_1中的正交补空间，$B|_{W_1}$是非退化的，$\dim W_1=r-1$。设η是U_1到U_2的等距变换，那么

$$U_2=\eta(U_1)=F(\eta\boldsymbol{u}_1)\perp F(W_1)=F\boldsymbol{u}_2\perp W_2,$$

其中$\eta(\boldsymbol{u}_1)=\boldsymbol{u}_2$，$\eta(W_1)=W_2$，$F\boldsymbol{u}_1\sim F\boldsymbol{u}_2$，$W_1\sim W_2$。由此得到

$$V=F\boldsymbol{u}_1\perp W_1\perp U_1^{\perp}=F\boldsymbol{u}_2\perp W_2\perp U_2^{\perp}。$$

利用$\dim U_1=1$的结果，有

$$W_1\perp U_1^{\perp}\approx W_2\perp U_2^{\perp}。$$

由于$\dim W_1=\dim W_2=r-1<r$，根据归纳法假设，得到$U_1^{\perp}\approx U_2^{\perp}$，综合上述，定理得证。通常称此定理为**维特消去定理**。

上面定理的证明，实际上给出了一个结果：两个非退化的子空间之间若有一等距变换，此变换可以扩张成为整个空间的正交变换。进而，去掉子空间非退化的条件，此结果仍然成立。

定理5.6.3 设Q是向量空间V上的非退化的二次型，U是

V 的子空间和 $\mathrm{rad}U=U\cap U^{\perp}\neq\{0\}$，$U=\mathrm{rad}U\oplus U'$，其中$U'$是$U$的子空间。令 $(z_1', \cdots, z_r)$ 是 $\mathrm{rad}U$ 的基底。那么可将U嵌入非退化子空间$U\oplus W$之中，其中W有基底 $(w_1, \cdots, w_r)$，使得 (z_i, w_i) 是双曲对，对所有 $1\leqslant i\leqslant r$，和

$$U+W=U'\perp H_1\perp\cdots\perp H_r,$$

其中 $H_i=Fz_i+Fw_i$，是一个双曲平面。

证明 令f是U上的线性函数，它由$f(z_1)=1$，对于 $2\leqslant i\leqslant r$；$f(z_i)=0$ 和对所有 $u'\in U$，$f(u')=0$ 给出。由命题 5.2.2，存在 $w_1\in V$ 使得 $f(u)=B(u, w_1)$，对所有 $u\in U$。于是 $f(z_1)=B(z_1, w_1)=1$，$f(z_i)=B(z_i, w_1)=0$，$2\leqslant i\leqslant r$，$B(u', w_1)=0$，对于所有 $u'\in U'$。如果 $Q(w_1)=0$，那么 (z_1, w_1) 是双曲对；如果 $Q(w_1)=a\neq 0$，令 $w_1'=-az_1+w_1$，(z_1, w_1') 是双曲对。以下设 (z_1, w_1) 是双曲对，设 $H_1=Fz_1+Fw_1$ 是双曲平面。由于 $B|_{H_1}$ 是非退化的，$V=H_1\oplus H_1^{\perp}$，$U_1=U'+\sum\limits_{j=2}^{r}Fz_j\subset H_1^{\perp}=V_1$ 和 $\mathrm{rad}\,U_1=\sum\limits_{j=2}^{r}F_j$。如果 $r=1$，$U+W=Fz_1+Fw_1+U'=H_1\perp U'$，$B|_{H_1}$ 和 $B|_{U'}$ 都是非退化的，因此 $B|_{U+W}$ 是非退化的，得到定理。如果 $r>1$，$V=H_1\perp V_1$。考虑 V_1 和 U_1，这时 $\dim U_1=r-1<r$。根据对 $\dim\ \mathrm{rad}U$ 进行归纳，可得 V_1 中的向量 $w_2, \cdots, w_r$，使得

$$U_1+\sum_{i=2}^{r}Fw_i=U'\perp H_2\perp\cdots\perp H_r, H_j=Fz_j+Fw_j。$$

那么 $W=\sum\limits_{i=1}^{r}Fw_i$ 满足定理条件。

定理5.6.4 设Q是V上非退化二次型。映射η是子空间U_1到子空间U_2的等距变换，那么η可以扩张为空间V的正交变换。

证明 分两种情况讨论：

(1) $\mathrm{rad}U_1=0$，即 U_1 是非退化子空间。由于 $U_1\approx U_2$，则

U_2也是非退化子空间。根据定理5.6.2，易见η可以扩张为V的正交变换。

（2）$\text{rad}U_1\neq 0$，$U_1=\text{rad}U_1\oplus U'_1$。根据定理5.6.3，存在子空间$W_1$，使得$U_1+W_1=U'_1\perp H_1\perp\cdots\perp H_r$，其中$H_i=Fz_i+Fw_i$，$z_i$，$w_i$是定理5.6.3中给出的，$U_1+W_1$是非退化的。令$\eta'|_{U_1}=\eta$，$\eta'(w_1)=w'_1$，$w'_1$是使得$(\eta z_1, w'_1)$成为双曲对的向量。于是

$$\eta'(U_1+W_1)=\eta'\left(U'_1+\sum_{i=1}^{r}Fz_i+\sum_{i=1}^{r}Fw_i\right)$$

$$=\eta'(U'_1)+\sum_{i=1}^{r}F\eta(z_i)+\sum_{i=1}^{r}w'_i$$

$$=\eta'(U'_1)\perp\eta'(H_1)\perp\eta'(H_2)\perp\cdots\perp\eta'(H_r),$$

其中$\eta'(H_i)=F\eta(z_i)+Fw'_i$。令$U_2=\eta'(U_1+W_1)$，$U_2$是非退化的和$U_1+W_1\sim U_2$，由定理5.6.2，$\eta'$可以扩张为$V$的正交变换，而$\eta'|_{U_1}=\eta$，于是$\eta$可以扩张为$V$的正交变换。

此定理通常称为**维特扩张定理**。

系5.6.1 若U_1和U_2是维数相同的全迷向子空间，则存在正交变换$\eta\in O(V,F)$，使得$\eta U_1=U_2$。

证明 由于$\dim U_1=\dim U_2$，存在将U_1映到U_2的可逆线性变换。设为η_1，因为U_1和U_2是全迷向的，η_1是等距的，即$U_1\overset{\eta_1}{\sim}U_2$。根据定理5.6.4，$\eta_1$可扩张为$V$的正交变换$\eta$，即$\eta\in O(V,F)$，而且$\eta U_1=U_2$。

所谓**极大全迷向子空间**是指一全迷向子空间，它不能真包含在更大的全迷向子空间之中。

系5.6.2 所有极大全迷向子空间有相同的维数。因此，极大全迷向子空间在正交群之下是可迁的。

证明 设U_1是任一全迷向子空间，U是极大全迷向子空间，则有$\dim U\geqslant\dim U_1$。如不然，即$\dim U<\dim U_1$，那么存在

$U_2 \subsetneqq U_1$，$\dim U_2 = \dim U$。于是存在$\eta \in O(V, Q)$，使得$\eta(U) = U_2$，$U = \eta^{-1}(U_2) \subsetneqq \eta^{-1}(U_1)$。$\eta^{-1}(U_1)$ 是全迷向子空间，这与U的极大性矛盾。

定义5.6.1 极大全迷向子空间的公共维数称为二次型Q的**维特指数**，用$\nu(Q)$表示。

系5.6.3 $\nu(Q) \leqslant \left[\frac{n}{2}\right]$，其中$\left[\frac{n}{2}\right]$表示$\frac{n}{2}$的最大整数部分。

证明 设U是极大全迷向子空间，$\dim U = \nu(Q) = \nu$，$\operatorname{rad} U = U$。由定理5.6.4，存在子空间W，使得

$$U + W = H_1 \perp H_2 \perp \cdots \perp H_\nu,$$

于是$2\nu \leqslant n$，即$\nu \leqslant \left[\frac{n}{2}\right]$。

对于空间V，可以分解为一些双曲平面和非迷向子空间的正交和。设U是V的极大全迷向子空间，$\dim U = \nu(Q) = \nu$；存在子空间W使得$U+W$是非退化的和$U + W = H_1 \perp \cdots \perp H_\nu$，$V = (U+W) \oplus (U+W)^\perp$。令$X = (U+W)^\perp$，则$X$是非迷向子空间。如不然，存在$x \in X$，$Q(x) = 0$。那么$U + Fx \supsetneqq U$和$U + Fx$是全迷向的，这与$U$的极大性矛盾。于是有$V$的分解

$$V = H_1 \perp H_2 \perp \cdots \perp H_\nu \perp X, \tag{5-20}$$

其中$\nu = \nu(Q)$，X是非迷向的。

系5.6.4 如果V除了式（5-20）外，还有分解式

$$V = H'_1 \perp \cdots \perp H'_r \perp Y, \tag{5-21}$$

其中H'_j是双曲平面，Y是非迷向的，那么有$\nu = r$和$X \approx Y$。

证明 取$z_i \in H'_i$，$1 \leqslant i \leqslant r$，是迷向向量，那么$\sum_{i=1}^{r} F z_i$是$r$维全迷向子空间，因此$r \leqslant \nu$。由于任何二个双曲平面都是等距的，再根据维特定理，可知存在$\eta \in O(V, Q)$，使得

$$\eta(H_1 \perp \cdots \perp H_r) = H'_1 \perp \cdots \perp H'_r$$

和 $$\eta(H_{r+1}\perp\cdots\perp H_r\perp X)=Y。$$

由于Y是非迷向的，有 $r=\nu$，$\eta(X)=Y$，即$X\approx Y$。

对于空间V的分解

$$V=H_1\perp\cdots\perp H_\nu\perp X,$$

选基底 $(z_1, w_1, z_2, w_2, \cdots, z_\nu, w_\nu, y_1, \cdots, y_t)$，其中 (z_i, w_i) 是双曲平面 H_i 的双曲对，$(y_1, \cdots, y_t)$ 是X的正交基，那么与Q相伴的对称双线性型的矩阵表示为

$$\begin{pmatrix} \left.\begin{matrix} 0 & 1 & & & & & \\ 1 & 0 & & & & & \\ & & 0 & 1 & & & \\ & & 1 & 0 & & & \\ & & & & \ddots & & \\ & & & & & 0 & 1 \\ & & & & & 1 & 0 \end{matrix}\right\}\nu\text{个} & \\ & C_2 \end{pmatrix},$$

其中 C_2 是可逆对角阵。由此可知，二次型的分类问题由维特指数 ν 和非迷向型所决定。对于 $\nu=\dfrac{n}{2}$，当然这时 n 为偶数，情况就简单多了。对此，适当排列基底，对称双线性型的矩阵表示为

$$\begin{pmatrix} 0 & I^{(\nu)} \\ I^{(\nu)} & 0 \end{pmatrix}。$$

这时可以将维特定理用矩阵的语言叙述如下。

定理5.6.2′ 两个$n\times n$可逆对称矩阵

$$\begin{pmatrix} C_1 & 0 \\ 0 & C_2 \end{pmatrix},\quad \begin{pmatrix} C_1 & 0 \\ 0 & C_3 \end{pmatrix}$$

合同，则 C_2 和 C_3 合同。

此定理的纯矩阵的证明，读者可参阅参考文献〔6〕。

利用定理5.6.2′，可以解决实数域上对称矩阵的合同问题。此问题作为练习请读者证明。

练习5.6.1 设S为实系数$n\times n$对称阵，则S合同于

$n\times n$阵

$$\begin{pmatrix} \left.\begin{matrix}1 & & \\ & \ddots & \\ & & 1\end{matrix}\right\}p & & \\ & \left.\begin{matrix}-1 & & \\ & \ddots & \\ & & -1\end{matrix}\right\}q & \\ & & \begin{matrix}0 & & \\ & \ddots & \\ & & 0\end{matrix} \end{pmatrix},$$

其中$p+q=r$是S的秩。更进一步，p和q由S唯一确定，称$p-q$为S的符号差。

由此，可以将维特指数理解为符号差概念的推广。

5.6.3 嘉当（E.Cartan）-狄多涅（Dieudonné）定理

这节主要讨论正交群的生成元。嘉当对于实数域或复数域上的二次型，证明了任何正交变换是至多n个对称的乘积，$n=\dim V$。这个结果由狄多涅推广到任意基域上的二次型。现先证明一个较弱的结果。

定理5.6.5 任何正交变换都是对称的乘积。

证明 设Q是向量空间V上的非退化的二次型，η是V上的正交变换，即$\eta\in O(V,Q)$。现对$\dim V=n$用归纳法来证明定理。若$\dim V=1$，由于Q是非退化的，任意取定$\boldsymbol{u}\neq 0$，都有$Q(\boldsymbol{u})\neq 0$，和$V=F\boldsymbol{u}$。$\eta\in O(V,Q)$，$\eta(\boldsymbol{u})=a\boldsymbol{u}$。由于$Q(\eta(\boldsymbol{u}))=Q(\boldsymbol{u})$，得到$a=\pm 1$。于是，如果$a=-1$，$\eta=S_u$；如果$a=1$，$\eta=S_u^2=1$。假设$\dim V<n$时定理成立，今证明$\dim V=n$时定理成立。观察消去定理的证明过程，可知存在$\boldsymbol{w}=\boldsymbol{u}+\epsilon\eta(\boldsymbol{u})$，$\epsilon=\pm 1$，适当选取$\epsilon=1$或$-1$，可使得$Q(\boldsymbol{w})\neq 0$和$S_w(\eta(\boldsymbol{u}))=-\epsilon\boldsymbol{u}$。令$\eta'=S_w\eta$，那么$\eta'(\boldsymbol{u})=-\epsilon\boldsymbol{u}$，于是$\eta'(F\boldsymbol{u})=F\boldsymbol{u}$，$\eta'(F\boldsymbol{u}^{\perp})=F\boldsymbol{u}^{\perp}$，和$Q|_{F\boldsymbol{u}^{\perp}}$是非退化的，$\dim F\boldsymbol{u}^{\perp}=n-1$。根据归纳法假设，$\eta'|_{F\boldsymbol{u}^{\perp}}=S'_{w_1}\cdots S'_{w_k}$，其中$\boldsymbol{w}_i\in F\boldsymbol{u}^{\perp}$。显然，$S_{w_i}|_{F\boldsymbol{u}^{\perp}}=S'_{w_i}$，$S_{w_i}(\boldsymbol{u})=\boldsymbol{u}$。令$\eta''=S_{w_1}\cdot S_{w_2}\cdots S_{w_k}$，$\eta''|_{F\boldsymbol{u}^{\perp}}=\eta'$，$\eta''(\boldsymbol{u})=\boldsymbol{u}$。如果$\epsilon=-1$，$\eta''(\boldsymbol{u})$

$=\eta'(\boldsymbol{u})$；如果 $\epsilon=1$，$\eta''(u)=S_u\eta'(\boldsymbol{u})$。因此 $\eta'=S_{w_1}\cdots S_{w_k}$ 或者 $\eta'=S_u\cdot S_{w_1}\cdots S_{w_k}$。于是得到 $\eta=S_v\cdot\eta'$ 是对称之积。

对于 $\eta\in O(V,Q)$，考虑关于 x 的线性函数

$$B(\eta(\boldsymbol{x}),\ \boldsymbol{y})=f_y(x)。$$

由于 B 是非退化的，存在 $y'\in V$，使得

$$f_y(\boldsymbol{x})=B(\boldsymbol{x},\ \boldsymbol{y}')=B(\eta(\boldsymbol{x}),\ \boldsymbol{y})。$$

考虑 V 上的变换 $\eta': y\to y'$，容易验证 η' 是线性的，而且是可逆的。由于 B 是对称的，

$$B(\eta(\boldsymbol{x}),\boldsymbol{y})=B(\boldsymbol{x},\ \eta'(\boldsymbol{y}))=B(\eta'(\boldsymbol{y}),\boldsymbol{x})$$
$$=B(\boldsymbol{y},\ (\eta')'(\boldsymbol{x}))=B((\eta')'(\boldsymbol{x}),\ \boldsymbol{y}),$$

于是 $\eta=(\eta')'$。由于 $\eta\in O(V,Q)$，有

$$B(\eta(\boldsymbol{x}),\ \boldsymbol{y})=B(\eta^{-1}(\eta(\boldsymbol{x}),\ \eta^{-1}(\boldsymbol{y}))$$
$$=B(\boldsymbol{x},\ \eta^{-1}(\boldsymbol{y}))。$$

因此 $\eta'=\eta^{-1}$。利用这个结果，可以证明下面练习。

练习5.6.2 设 $\eta\in O(V,\ Q)$，令集合

$$V_1=\{\boldsymbol{x}\in V\mid\eta(\boldsymbol{x})=\boldsymbol{x}\},$$

则 $V_1=((1-\eta)V)^{\perp}$。

对于线性变换 T，如果 $T-I$ 是幂零的，通常称 T 为**幺幂零**的。关于幺幂零的线性变换，有下面的性质。

命题5.6.1 如果线性变换 T 是幺幂零的，则 $\det T=1$。

证明 对 $\dim V$ 采用归纳法来证明命题。若 $\dim V=1$，命题显然成立。假设命题对 $\dim V<n$ 成立，今证明它对 $\dim V=n$ 也成立。设 $T-I=Z$，Z 是幂零的，选取正整数 l，使得 $Z^l=0$ 和 $Z^{l-1}\neq 0$。于是存在 $\boldsymbol{v}\in V$，使得 $Z^{l-1}\boldsymbol{v}=\boldsymbol{u}\neq 0$，但是 $Z\boldsymbol{u}=0$，即 $T\boldsymbol{u}=\boldsymbol{u}$。于是 $T|_{F\boldsymbol{u}}=I$，是恒等变换。令 $V_1=V/F\boldsymbol{u}$，$\dim V_1=n-1$。T 在 V_1 上诱导出线性变换 T_1，$T_1(\boldsymbol{v}+F\boldsymbol{u})=T\boldsymbol{v}+F\boldsymbol{u}$。$T_1$ 在 V_1 是幺幂零的，由归纳法假设 $\det T_1=1$，设 $(\boldsymbol{u}_2+F\boldsymbol{u},\ \cdots,\ \boldsymbol{u}_n+F\boldsymbol{u})$ 是 V_1 的基底，那么 $(\boldsymbol{u}_1=\boldsymbol{u},\cdots,\ \boldsymbol{u}_n)$ 是 V 的基底，T 相对此基底的阵表示为

$$\begin{pmatrix} 1 & 0 & \cdots & 0 \\ a_{21} & a_{22} & \cdots & a_{2n} \\ & \cdots & \cdots & \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix},$$

其中

$$\begin{pmatrix} a_{22} & \cdots & a_{2n} \\ & \cdots\cdots & \\ a_{n2} & \cdots & a_{nn} \end{pmatrix}$$

是 T_1 相对（$\boldsymbol{u}_2+F\boldsymbol{u}$, $\cdots$, $\boldsymbol{u}_n+F\boldsymbol{u}$）的阵表示。因此得到 $\det T=1$。

定理5.6.6（嘉当-狄多涅）定理 如果 $\dim V=n$，则 V 上的任何正交变换 η 是至多 n 个对称的乘积。

证明 分几种情况讨论。

（1）假设 η 的固定点空间 V_1,

$$V_1=\{\boldsymbol{v}\in V \mid \eta(\boldsymbol{v})=\boldsymbol{v}\},$$

不是全迷向子空间，因此存在 $\boldsymbol{u}\in V_1$，使得 $Q(\boldsymbol{u})\neq 0$，和 $V=F\boldsymbol{u}\perp(F\boldsymbol{u})^{\perp}$。令 $\eta|_{(F\boldsymbol{u})^{\perp}}=\eta_1$，$Q|_{(F\boldsymbol{u})^{\perp}}$ 是非退化的，由归纳法假设，η_1 是至多（$n-1$）个对称之积。设 $\eta_1=S_{\boldsymbol{w}_1}\cdots S_{\boldsymbol{w}_r}$，$r\leqslant n-1$，$\boldsymbol{w}_i\in(F\boldsymbol{u})^{\perp}$，于是

$$\eta=S_{\boldsymbol{w}_1}\cdots S_{\boldsymbol{w}_r}。$$

（2）如果存在 $\boldsymbol{u}\in V$，使得 $Q(\boldsymbol{u})\neq 0$ 和 $Q(\boldsymbol{u}-\eta(\boldsymbol{u}))\neq 0$，定理也成立。因为在维特消去定理的证明过程中，曾得到

$$\eta'=S_{\boldsymbol{w}}\cdot\eta,\quad \eta'(\boldsymbol{u})=\boldsymbol{u},$$

其中 $\boldsymbol{w}=\boldsymbol{u}-\eta(\boldsymbol{u})$。于是 $\boldsymbol{u}$ 属于 η' 的固定子空间，由（1）的结果可知，η' 是至多（$n-1$）个对称之积。因此 $\eta=S_{\boldsymbol{w}}\cdot\eta'$ 是至多 n 个对称之积。

（3）设 $\dim V=2$。如果 Q 是非迷向的，即空间 V 中没有迷向向量，那么由（1）和（2）的结果便得到定理。因此，下面假设 V 是双曲平面。在定理5.6.1中已经看到，对于 V 的双曲对 $(\boldsymbol{u},\boldsymbol{v})$，$\eta(\boldsymbol{u})=a\boldsymbol{u}$，$\eta(\boldsymbol{v})=a^{-1}\boldsymbol{v}$ 或者 $\eta(\boldsymbol{u})=a\boldsymbol{v}$，$\eta(\boldsymbol{v})=$

$a^{-1}\cdot \boldsymbol{u}$。在第一种情况，可假设 $a\neq 1$，否则 $\eta=1$，是单位变换。令 $\boldsymbol{w}=\boldsymbol{u}+\boldsymbol{v}$，$\boldsymbol{w}$ 满足 $Q(\boldsymbol{w})\neq 0$ 和 $Q(\boldsymbol{w}-\eta(\boldsymbol{w}))\neq 0$，这正是（2）。在第二种情况，令 $\boldsymbol{w}=\boldsymbol{u}+a\boldsymbol{v}$，则 $\eta(\boldsymbol{w})=\boldsymbol{w}$，和 $Q(\boldsymbol{w})\neq 0$，这便是（1）。

（4）设 $\dim V\geqslant 3$ 和 η 的固定点空间 V_1 是全迷向的，而且对于 $Q(\boldsymbol{u})\neq 0$ 的任何 $\boldsymbol{u}$ 都有 $Q(\boldsymbol{u}-\eta(\boldsymbol{u}))=0$。事实上，对于 $\dim V\geqslant 3$，对每个 $\boldsymbol{u}\in V$ 都有 $Q(\boldsymbol{u}-\eta(\boldsymbol{u}))=0$。为此，只要对于 $\boldsymbol{w}\neq 0$ 和 $Q(\boldsymbol{w})=0$ 有 $Q(\boldsymbol{w}-\eta(\boldsymbol{w}))=0$。考虑 $F\boldsymbol{w}^{\perp}$，因为 B 是非退化的，$\dim F\boldsymbol{w}^{\perp}=n-1$。由于 $n\geqslant 3$，$n-1>\left[\frac{n}{2}\right]=\nu(Q)$，所以 $F\boldsymbol{w}^{\perp}$ 不是全迷向的。因此，存在向量 $\boldsymbol{u}\neq 0$，$\boldsymbol{u}\perp\boldsymbol{w}$ 和 $Q(\boldsymbol{u})\neq 0$。于是 $(\boldsymbol{u}\pm\boldsymbol{w})\perp\boldsymbol{w}$ 和 $Q(\boldsymbol{w}\pm\boldsymbol{u})=Q(\boldsymbol{u})\neq 0$。令 $\zeta=1-\eta$，得到 $Q(\zeta(\boldsymbol{u}))=0$，$Q(\zeta(\boldsymbol{w})+\zeta(\boldsymbol{u}))=0$，$Q(\zeta(\boldsymbol{w})-\zeta(\boldsymbol{u}))=0$。由此可得 $Q(\zeta(\boldsymbol{w}))=Q(\boldsymbol{w}-\eta(\boldsymbol{w}))=0$。这表明 $(1-\eta)V$ 是全迷向子空间。由练习 5.6.2，$V_1=((1-\eta)V)^{\perp}$，因此 $V_1^{\perp}=(1-\eta)V$。V_1 和 $(1-\eta)V$ 都是全迷向的和 $V_1\subset V_1^{\perp}=(1-\eta)V$，$(1-\eta)V\subset((1-\eta)V)^{\perp}=V_1$，因此 $V_1=(1-\eta)V=V_1^{\perp}$，对任何向量 $\boldsymbol{x}\in V$，$(1-\eta)^2\boldsymbol{x}=0$，即 η 是幺幂零的，有 $\det\eta=1$，$n=\dim V=\dim V_1+\dim V_1^{\perp}$。由于 $V_1=V_1^{\perp}$，n 必定是偶数。令 $\eta'=S_w\eta$，其中 S_w 是任何对称。η' 是非正常的，观察定理 5.6.5 的证明过程，可以得到 η' 是 $k\leqslant n$ 个对称之积。由于 k 是奇数，n 是偶数，有 $k\leqslant n-1$。因此 $\eta=S_w\eta'$ 是 $\leqslant n$ 个对称之积。得到定理。

系5.6.5 奇数维向量空间上的任何旋转和偶数维向量空间上的任何非正常正交变换都有非零固定点。

证明 设正交变换 $\eta=S_{u_1}\cdots S_{u_k}$，$k\leqslant n=\dim V$，其中 S_{u_i} 是由 $\boldsymbol{u}_i$ 决定的对称。S_{u_i} 的固定点集合是一个 $(n-1)$ 维的超平面 U_i，这 k 个超平面的交显然包含在 η 的固定点集合之中。设 η 是满足定理条件的正交变换，那么 $k\leqslant n-1$。由熟知的维数

定理：$\dim(U_1\cap U_2)=\dim U_1+\dim U_2-\dim(U_1+U_2)$，其中 U_1 和 U_2 是任何两个子空间，可以推出

$$\dim\left(\bigcap_{i=1}^{n-1} U_i\right)\geqslant n-(n-1)=1,$$

这里的 U_i 是指超平面。由此，η 有非零固定点。

特别，3 维实数域上的欧几里得空间的旋转有非零固定点。

定理5.6.7 如果 $\dim V\geqslant 3$，则

$[O(V,Q),\ O(V,Q)]=[O^+(V,Q),\ O^+(V,Q)]$。

证明 设所有 $(S_u\cdot S_v)^2$ 生成的子群为 $O'(V,Q)=O'$，即

$$O'(V,Q)=\langle(S_uS_v)^2|\boldsymbol{u},\ \boldsymbol{v}\in V,\ Q(\boldsymbol{u})\neq 0,\ Q(\boldsymbol{r})\neq 0\rangle。$$

由于 $\eta S_u\eta^{-1}=S_{\eta(u)}$，对于 $\eta\in O(V,Q)$，因此 $O'\lhd O(V,Q)$，而且 $O(V,Q)/O'(V,Q)$ 是交换群，于是 $O'(V,Q)\supseteq[O(V,Q),\ O(V,Q)]$。反方向的包含关系是显然的。因此 $O'[V,Q]=[O(V,Q),\ O(V,Q)]$。为了证明定理，只需证明任何 $(S_uS_v)^2$ 是旋转换位子的乘积就够了。若 $n=\dim V$ 是奇数，$(-1)S_u$ 是旋转，和 $(S_uS_v)^2=((-S_u)\cdot(-S_v))^2$。若 $n=\dim V$ 是偶数，则 $n\geqslant 4$。令 $U=F\boldsymbol{u}+F\boldsymbol{v}$，则存在 $\boldsymbol{w}\in U^\perp$，使得 $Q(\boldsymbol{w})\neq 0$。如不然，$U^\perp$ 是全迷向的，有 $(U^\perp)\subset(U^\perp)^\perp=U$。由于 $\dim U^\perp=n-\dim U\geqslant n-2\geqslant 2$，有 $U=U^\perp$，U 是全迷向的，这与 $Q(\boldsymbol{u})\neq 0$，$\boldsymbol{u}\in U$ 矛盾。考虑 $S_uS_wS_u^{-1}=S_w$，因此 $S_uS_w=S_wS_u$。类似地有 $S_vS_w=S_wS_v$，于是 $[S_u,S_v]=[S_uS_w,S_vS_w]$。定理得证。

典型群的内容非常丰富，由于篇幅所限，这里只给出最基本的结果，而且没讨论酉群。对于典型群进一步结果有兴趣的读者可参见参考文献[5，6，9]。

参考文献

1 Cotton F A. Chemical Applications of Group Theory. John Wiley & Sons, Inc., 1971

2 Curtis C W and Reiner I. Representation Theory of Finite Groups and Associative Algebra. John Wiley & Sons, Inc., 1962

3 Gardiner C. F. A First Course in Group Theory. Springer-Verlag New York Inc., 1980

4 Hall M and Senion J K. The Groups of Order 2^n, $n \leqslant 6$. New York: Macmillans, 1964

5 Jacobson N. Basic Algebra I. W H Freeman and Company, 1974

6 华罗庚 万哲先. 典型群. 上海：上海科学技术出版社，1963

7 Johnson D L. Presentations of Groups. London: C. U. P., 1976

8 Miller M. Symmetric Groups and Their Applications. New York: Academic Press, 1972

9 O'Meara O T. Symplectic Groups. Providence, R. I., 1978

10 Yala P B. Geometry and Symmetry. San Francisco: Holden-Day, 1968

11 严志达 许以超. Lie群及其Lie代数. 北京：高等教育出版社，1985

12 邦德列雅金 Л C. 连续群. 曹锡华. 北京：科学出版社，1978

[General Information]
书名=群论
作者=刘木兰　冯克勤
页数=189
SS号=10101770
出版日期=1992年07月第1版

前言
目录
第一章　群和它的基本性质
　　１．１　集合论的预备知识
　　１．２　什么是群
　　１．３　子群和陪集分解
　　１．４　循环群
　　１．５　正规子群　商群　同态定理
第二章　群在集合上的作用　西洛（Ｓｙｌｏｗ）定理
　　２．１　置换群
　　２．２　群在集合上的作用
　　２．３　西洛定理
第三章　群的结构
　　３．１　自由群和群的表现
　　３．２　有限生成阿贝尔群结构
　　３．３　小阶群的结构
　　３．４　幂零群和可解群
第四章　有限点群
　　４．１　三维空间中的正交群
　　４．２　欧几里得群
　　４．３　Ｅ（３）的离散子群
　　４．４　正多面体和它们的对称群
　　４．５　第一类点群
　　４．６　第二类点群
　　４．７　晶体点群
第五章　典型群
　　５．１　线性群的结构
　　５．２　双线性型
　　５．３　交错型
　　５．４　辛群
　　５．５　二次型和对称双线性型
　　５．６　正交群
参考文献